Forest Service Manual
National Headquarters - Washington Office
Washington, DC

Forest Service Manual 6600 – System Management
Chapter 6680 – Cybersecurity of Information, Information Systems, And Information Technology

Amendment: 6600-2024-1

Effective date: January 17, 2024

Duration: This amendment is effective until superseded or removed.

Approved by: Antoine Dixon, Deputy Chief, Business Operations

Date approved: January 12, 2024

Responsible Staff: Capital Planning & Information Technology Governance (CPITG)

Last Change:

Superseded Document(s): 6680-6685, Amendment 6600-2021-1, November 22, 2021

Digest: Following is an explanation of the changes throughout the directive by section.

6680.01b – Updates references throughout section.

6680.01c – Adds reference to the Federal Acquisitions Regulations (FAR).

6680.01d – Updates referenced Government-wide directives and standards.

6680.01f, 6680.01g – Updates United States Department of Agriculture (USDA) policies.

6680.05 – Adds new definitions and removes obsolete definitions. Revises the definition of "annual" to mean "once per calendar year" instead of "once per fiscal year". Revises Information Technology (IT) definition to include the Internet of Things (IoT).

6680.06a – Revises National Institute of Standards and Technology (NIST) Publication table.

6682.04 and throughout document – Updates references to the USDA Risk Management Framework (USDA RMF).

6682.04d – Adds Authorizing Official responsibility for ensuring that information systems used to conduct or host information collected from the public require security controls

commensurate with the appropriate Federal Information Security Modernization Act (FISMA) compliance level(s) and are properly authorized prior to collection.

Also adds Authorizing Official responsibility for ensuring the implementation of USDA Information and Communication Technology Supply Chain Risk Management (ICT SCRM) strategy and approving mitigation plans for SCRM residual risks in accordance with USDA Departmental Notice (DN) 3540-004 or other USDA guidance.

6682.1 – Adds policy requirement to ensure the security categorization of any system processing, storing, or transmitting controlled unclassified information (CUI) is at least moderate confidentiality impact level.

6682.3 – Adds policy requirement in the System Development Life Cycle Security Planning to use Zero Trust Architecture (ZTA) principles whenever possible.

6683.04 – Changes incident reporting responsibilities.

6683.04m – Changes responsibilities for devices while on international travel from just employees to all end users.

6683.23g – Changes the requirement for reimaging devices from “will be reimaged” to “may be reimaged”.

6685.04n – Changes responsibility of System Owners to incorporate the System Privacy Plan into the System Security Plan (SSP) unless otherwise directed.

Table of Contents

6680.01 - Authority

6680.01a - Laws

1. *Chief Financial Officer Act of 1990 (Pub. L 101-576)*. This Act requires that the Forest Service Chief Financial Officer comply with applicable accounting principles, standards, and requirements and with internal control standards; to provide complete, reliable, consistent, and timely information.

2. *Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501-6506).* This Act applies to the online collection of personal information by persons or entities under U.S. jurisdiction from children under 13 years of age. It details what a web site operator shall include, in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator has to protect for children's privacy and safety online, including restrictions on marketing to children under 13 years of age. The Federal Trade Commission has the authority to issue regulations and enforce the Act.

3. *Clinger-Cohen Act, formerly known as the Information Technology Management Reform Act of 1996 (41 U.S.C. 251)*. This Act updates and defines how the Federal Government may acquire and dispose of information technology.

4. *E-Government Act of 2002*. This Act was signed into law on December 17, 2002. "Electronic Government" is defined as the Government use of "web-based Internet applications or other information technology to enhance the access to and delivery of government information and services to the public, other agencies, and other Government entities; or to bring about improvements in Government operations that may include effectiveness, efficiency, service quality, or transformation." Its stated purpose is to improve the management and promotion of electronic government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget (OMB), and by establishing a framework of measures that require using Internet-based information technology to improve citizen access to government information and services, and for other purposes. It specifically addresses the requirements for implementing Privacy Impact Assessments (PIAs) for Federal systems.

5. *Federal Information Security Modernization Act (FISMA) of 2014 (Pub. L. 113-283; 44 U.S.C. 3541-3549)*. This Act sets minimum information security requirements, requires agencies to implement information security protections commensurate with the magnitude of harm that could result from a security incident, and requires sufficient training for all personnel.

6. *Federal Managers' Financial Integrity Act of 1982 (Publication L. 97-255; 96 Stat. 814)*. This Act requires that the Office of Management and Budget (OMB) evaluate agencies' accounting and administrative control systems and that agencies self-evaluate those systems.

7. *Privacy Act of 1974 (5 U.S.C. 552).* This Act directs agencies to safeguard the privacy of individuals by only disclosing records to others for certain purposes or with an individual's written consent; provides individuals with access to and the means to amend their records; establishes exemptions by which access, or amendment may be denied; and provides an appeal process when requests for access or amendment are denied. Also, requires that agencies inform appellants of their right to file a concise statement and the provisions thereof, and to inform them of their right to seek judicial review.

8. *Rehabilitation Act of 1973 (29 U.S.C. 501-508)*. This Act prohibits discrimination against people with disabilities, applies to programs conducted by Federal agencies; those receiving Federal funds, such as colleges participating in Federal student loan programs; Federal employment; and employment practices of businesses with Federal contracts. The standards for determining employment discrimination under the Rehabilitation Act are the same as those used in Title I of the Americans with Disabilities Act.

9. *The Paperwork Reduction Act of 1995 (44 U.S.C. 3501)*. This Act mandates promoting the use of information technology to improve the productivity, efficiency, and effectiveness of Forest Service programs, and requires development and implementation of policies, principles, standards, and guidelines for information technology functions and activities. Requires OMB to approve information collections that will be conducted with 10 or more members of the public over a 12-month period.

10. *Title 5, United States Code, section 301 (5 U.S.C. 301).* This Code provides that the head of an executive department or military department may prescribe regulations for the use of its property.

11. *Title 18, United States Code, section 1030 (18 U.S.C. 1030).* This Code prohibits unauthorized access to and use of Government computer systems.

6680.01b - Executive Orders

1. *Executive Order 12968, Access to Classified Information*. This Order was issued August 2, 1995 and establishes a uniform Federal personnel security program for employees who will be considered for initial or continued access to classified information.

2. *Executive Order 13467, Security Requirements for Government Employment.* This Order was issued June 30, 2008 and specifies particular criteria and responsibilities for investigating the background and character of individuals employed or seeking employment in the Federal Government to ensure that the interests of national security are met.

3. *Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain*. This order was issued on May 17, 2019 and focused on securing the information and communications technology and services supply chain against transactions involving "foreign adversaries."

4. *Executive Order 14028, Improving the Nation's Cybersecurity.* This order was issued on May 12, 2021 and removes barriers to threat information sharing between Government and the private sector, helps move the Federal Government to secure cloud services and a zero-trust architecture, mandates deployment of multifactor authentication and encryption within a specific time period and improves the supply chain security of software by establishing baseline security standards for development of software sold to the Government.

5. *Executive Order 14034, Protecting Americans' Sensitive Data from Foreign Adversaries.* This order was issued on June 11, 2021 and elaborates upon measures to address the national emergency with respect to the information and communications technology and services supply chain that was declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain). This executive order identifies factors that may be considered in evaluating the risks of connected software applications under the Executive Order 13873 framework.

6680.01c - Regulations

1. *Title 5, Code of Federal Regulations, Part 731, Office of Personnel Management - Suitability*. This Code requires that every competitive service position have a risk determination and requires some specific procedural strategies, such as background investigations.

2. *Title 5, Code of Federal Regulations, Part 732, Office of Personnel Management - National Security Positions*. This Code defines sensitivity level designations and investigative requirements for positions determined to be sensitive to national security.

3. *Title 5, Code of Federal Regulations, Part 736, Personnel Investigations*. This Code describes the investigation process for Federal employees.

4. *Title 5, Code of Federal Regulations, Part 930, subpart C, Information Security Responsibilities for Employees Who Manage or Use Federal Information Systems*. This Code requires initial, continued, and refresher security training for Forest Service employees responsible for the management or use of computer systems that process sensitive information.

5. *Title 5, Code of Federal Regulations, Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch, section 2635.702*. This Code prohibits use of public office for private gain.

6. Title 7, Code of Federal Regulations, section 2.60 (a) (27). This Code sets out the delegation to the Forest Service to administer radio spectrum management for the USDA.

7. *Title 48, Code of Federal Regulations, Chapter 1, Federal Acquisition Regulation (FAR) System*. Chapter 1 of Title 48 of this Code is government-wide acquisition regulations and includes supply chain and cybersecurity acquisition requirements.

6680.01d - Government-wide Directives and Standards.

1. *Federal Continuity Directive 1, January 2017*. This Directive describes the key elements of a viable continuity capability and the importance of coordinating with non-Federal organizations to establish and maintain a comprehensive and effective national continuity capability.

2. *Federal Continuity Directive 2, June 2017*. This Directive provides implementation guidelines for the requirements identified in Federal Continuity Directive 1, Annex C.

3. *General Accountability Office, Federal Information Systems Controls Audit Manual, 2009*. This Manual describes the control activities, control techniques, and audit procedures for evaluating the separation of duties principles used in Federal agencies. It provides guidance to auditors in evaluating internal controls over the integrity, confidentiality, and availability of maintained data.

4. *Office of Management and Budget Circular A-123, Management's Responsibility for Internal Control*. Circular A-123 provides guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls.

5. *Office of Management and Budget Circular A-130*. Circular A-130 establishes general policy for information governance, acquisitions, records management, open data, workforce, security, and privacy. It also emphasizes the role of both privacy and security in the Federal information life cycle. It includes Appendix I, Responsibilities

for Protecting and Managing Federal Information Resources, and Appendix II, Responsibilities for Managing Personally Identifiable Information.

6. *Office of Management and Budget Memorandum 17-12, Preparing for and Responding to the Breach of Personally Identifiable Information*. This Memorandum establishes requirements to safeguard PII, to develop rules of conduct for handling PII, and to develop procedures for responding to and reporting PII breaches, and for external breach notification procedures.

7. *Office of Management and Budget Memorandum M-21-30, Protecting Critical Software Through Enhanced Security Measures*. This Memorandum defines Critical Software and provides instructions for the implementation of fundamental measures required to secure its use.

8. *Office of Management and Budget Memorandum M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response* (EDR). This memorandum provides implementation guidance to agencies as they accelerate the adoption of EDR solutions and work to improve visibility into and detection of cybersecurity vulnerabilities and threats to the Government, as defined in EO 14028.

9. *Office of Management and Budget Memorandum M-22-05. Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*. This Memorandum provides agencies with fiscal year (FY) 2021-2022 reporting guidance and deadlines in accordance with the Federal Information Security Modernization Act of 2014 (FISMA).

10. *Office of Management and Budget Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. This Memorandum sets forth a Federal zero trust architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives.

11. *Homeland Security Presidential Directive 7, Critical Infrastructure Identification, Prioritization, and Protection*. This Directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure, key resources, and to protect them from terrorist attacks.

12. *Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors*. This Directive requires the establishment of a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

13. *Homeland Security Presidential Directive 20, National Continuity Policy*. This Directive establishes a comprehensive national policy on the continuity of Federal Government structures and operations, and also creates the position of a single National Continuity Coordinator responsible for coordinating the development and implementation of Federal continuity policies. This policy establishes "National Essential Functions," prescribes continuity requirements for all executive departments and agencies, in order to ensure a comprehensive and integrated national continuity program that will enhance the credibility of our national security posture and enable a more rapid and effective response to and recovery from a national emergency.

6680.01e - U.S. Department of Agriculture Directives

1. *Department Personnel Manual, Chapter 751, Discipline.* This Manual provides guidelines for disciplinary action.

6680.01f - Departmental Manuals

1. *Departmental Manual 3300-026, Planning and Managing Wireless Technologies*. This Manual establishes USDA policy for planning and managing USDA's wireless networks and devices that use USDA wireless networks.

2. *Departmental Manual 3505-005, Cybersecurity Incident Management Procedures*. This Manual provides guidance for cybersecurity incident management and reporting and describes essential preparations for effective incident management.

3. *Departmental Manual 3510-001, Chapter 2, Part I, Physical Security Standards for Information Technology (IT) Restricted Space*. This Manual directs that information technology restricted space be considered part of the Forest Service's critical infrastructure and provides detailed guidance for physically securing facilities containing critical information technology infrastructure and for identifying, reporting, mitigating, and correcting deficiencies.

4. *Departmental Manual 3530-004, Firewall Technical Security Standards*. This Manual requires the use of firewalls between Forest Service and USDA networks and the use of secure Internet protocol (IP) connectivity from the Internet to USDA networks. This policy also details procedures, including equipment and services, for meeting those requirements.

5. *Departmental Manual 3530-005, Encryption Security Standards*. This Manual provides direction to all USDA agencies and staff offices to use the Approved Protocols and Protection Techniques.

6. *Departmental Manual 3545-002, Information Systems Security Program*. This Manual requires agencies to organize, implement and maintain an Information Systems Security Program that ensures security of all information technology assets.

7. *Departmental Manual 3560-001, Security Requirements for Capital Planning and Investment Control (CPIC)*. This Manual requires all USDA agencies and staff offices to institute a formal CPIC process and execute all CPIC responsibilities for both the overall security program and all major IT investments.

8. *Departmental Manual 3575-001, Security Controls in the Systems Life Cycle/Systems Development Life Cycle*. This Manual requires USDA agencies and staff offices to select a systems development life cycle and implement the appropriate baseline security controls during the life of all information technology systems.

9. *Departmental Manual 4620-002, Common Identification Standard for U.S. Department of Agriculture (USDA)*. This Manual provides procedures for USDA staff to meet the Personal Identity Verification (PIV) requirements.

10. *Departmental Manual 9610-002, USDA Security Policies and Procedures for Laboratories and Technical Facilities (Excluding Biosafety Level 3 Facilities)*. This Manual establishes policy for the security of critical assets.

6680.01g - Departmental Regulations

1. *Departmental Regulation 1800-001, Incident Preparedness, Response, and Recovery*. Regulation 1800-001 describes the incident preparedness, response, and recovery responsibilities, designates the Mission Areas, agencies, and staff offices that will carry out these responsibilities, and includes Continuity of Operations (COOP).

2. *Departmental Regulation 3140-001, USDA Information Systems Security Policy*. Regulation 3140-001 directs all USDA agencies to design, implement, and maintain an adequate security program for information resources; establishes guidelines for system usage; and requires implementation of comprehensive information protections, including individual accountability, throughout the Forest Service functions and mandates the practice of separation of duties to the extent possible.

3. *Departmental Regulation 3140-002, Internet Security Policy*. Regulation 3140-002 directs all USDA agencies to develop and implement an Internet security policy, establishes minimum security requirements, and identifies some prohibited uses.

4. *Departmental Regulation 3145-001, Oversight and Management of the Federal Information Technology Acquisition Reform Act*. Regulation 3145-001 establishes the USDA policy governing the oversight and management of the Federal Information Technology Acquisition Reform Act (FITARA), Public Law (P.L.) 113-291.

5. *Departmental Regulation 3170-001, End User Workstation Configurations*. Regulation 3170-001 establishes policy for approved workstations and associated peripheral configurations for all users within the USDA.

6. *Departmental Regulation 3180-001, Information Technology Standards*. Regulation 3180-001 establishes the standards for the acquisition, configuration, and administration of information technology within the USDA.

7. *Departmental Regulation 3300-001, Telecommunications & Internet Services and Use.* Regulation 3300-001 provides authority for information resource management and provides guidelines for electronic mail and Internet use.

8. *Departmental Regulation 3410-001, Information Collection Request Activities: Collection of Information from the Public.* Regulation 3410-001 establishes USDA policy for the management requirements associated with the clearance of an information collection request, including proper accreditation of the information system that will be used to conduct or host the collected information prior to the start of information collection.

9. *Departmental Regulation 3440-003, Controlled Unclassified Information (CUI) Program.* Regulation 3440-003 establishes the USDA program office for Controlled Unclassified Information (CUI) and begins program implementation.

10. *Departmental Regulation 3450-001, Computer Matching Program Involving Personally Identifiable Information."* Regulation 3450-002 establishes policy and defines roles and responsibilities for conducting USDA's Computer Matching Program. This DR also addresses the use of computerized comparisons of two or more automated information systems for establishing and verifying Federal benefit program eligibility or recouping payments, delinquent debts, or overpayments owed to Government Agencies from a Federal benefit program

11. *Departmental Regulation 3505-003, Access Control for Information and Information Systems*. Regulation 3505-003 establishes the USDA policy for implementing, managing, and enforcing logical access to information systems and granting accounts the least privileges necessary to carry out assigned duties or actions.

12. *Departmental Regulation 3505-005 Cyber Security Incident Management*. Regulation 3505-005 establishes the USDA policy for preparing for, responding to, and reporting cybersecurity incidents.

13. *Departmental Regulation 3515-001, Use of Web Measurement and Customization Technologies*. Regulation 3515-001 establishes guidance for the use of web measurement and customization technologies and the associated privacy

requirements for public-facing and external websites and applications owned or operated on behalf of USDA.

14. *Departmental Regulation 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII)*. Regulation 3515-002 establishes the USDA privacy policy, provides the impetus and foundations for the Privacy Program, and guides the development of associated processes and procedures.

15. *Departmental Regulation 3520-002, Configuration Management*. Regulation 3520-002 establishes the USDA policy for configuration management, security configuration management, which is also known as secure or security-focused configuration management, and inventory management.

16. *Departmental Regulation 3540-003, Security Assessment and Authorization*. Regulation 3540-003 establishes the Security Assessment and Authorization (A&A) policy of the USDA for meeting the applicable laws, regulations, and standards of the Federal Government.

17. *Departmental Regulation 3545-001, Information Security Awareness and Training Policy*. Regulation 3545-001 requires agencies to develop, implement, and maintain an information technology security awareness and training program to ensure the security of information systems.

18. *Departmental Regulation 3545-003, Suitability Requirements Permitting Personnel Access to Information Systems*. Regulation 3545-003 provides the policy for assessing the suitability of personnel to access USDA information resources, establishes the criteria for personnel to gain and maintain access to USDA information and information systems, and defines the standards by which personnel establish and maintain a level of trust.

19. *Departmental Regulation 3565-003, Plan of Action and Milestone Policy.* Regulation 3565-003 establishes USDA policy for identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security vulnerabilities found in USDA programs, applications, and systems.

20. *Departmental Regulation 3571-001, Information System Contingency Planning and Disaster Recovery Planning.* Regulation 3580-004 establishes USDA policy to guide agencies and staff offices in developing, implementing, and maintaining Information System Contingency Plans (ISCPs) and facility Disaster Recovery Plans (DRPs).

21. *Departmental Regulation 3575-003, Information Systems Log Retention Requirements.* Regulation 3575-003 establishes USDA requirements for retaining, maintaining, and allowing access to information system logs.

22. *Departmental Regulation 3580-004, Securing Remote Access to USDA Information Systems and Client Devices.* Regulation 3580-004 establishes policy for secure remote access to USDA information systems with secure devices.

23. *Departmental Regulation 3580-005, Securing Client Devices for International Travel*. Regulation 3580-004 establishes the policy for secure remote access to USDA information and information systems prior to, during, and upon return from foreign locations.

24. *Departmental Regulation 3640-001, Identity, Credential, and Access Management.* Regulation 3640-001 establishes policies related to identity, credential, and access management for unclassified systems in the USDA.

25. *Departmental Regulation 3650-001, Cloud Computing.* Regulation 3650-001 establishes the USDA policy for implementing the Federal Cloud Computing Initiative across the USDA's information technology (IT) portfolio of information and information systems.

26. *Departmental Regulation 4070-735-001, Employee Responsibilities and Conduct*. Regulation 4070-735-001 provides requirements for all USDA employees in a variety of areas related to employee conduct; section 16 addresses use of computers.

27. *Departmental Regulation 4080-811-02, USDA Telework Program.* Regulation 4080-811-001 sets forth the authority, policy, and responsibilities for managing the Telework and Remote Work Programs within the USDA.

6680.02 - Objectives

1. Evaluate, regulate, and monitor the effectiveness of security controls that safeguard IT resources that support the Forest Service mission.

2. Maintain ongoing awareness of information security, vulnerabilities, assets, and threats in support of the Forest Service information security policy for systems storing or processing Forest Service information and in accordance with National Institute of Standards and Technology (NIST) guidelines.

6680.03 - Policy

1. Implement and monitor appropriate security controls at all levels of the Forest Service to protect the confidentiality, integrity, and availability of the information, information systems, and IT that supports the Forest Service mission.

2. Include appropriate provisions in contracts, agreements with cooperators, and other instruments to ensure that non-Forest Service personnel who work with Forest Service information, information systems, and IT follow requirements for

appropriate use and security of Forest Service-owned and leased information resources as set out for employees in the Forest Service Directive System and other authorities (FSM 6680.1).

3. Allow exceptions to the requirements in FSM 6680 in accordance with risk-based decision (RBD) and approval by the information system Authorizing Official (AO).

4. Implement this policy, within 6 months of issuance for existing system and immediately for new systems, by following standard CIO-approved procedures.

6680.04 - Responsibility [Reserved]

6680.05 - Definitions

Access. A connection between users, or processes acting on behalf of users, and devices, files, records, processes, programs, domains, or other objects in an information system that allow reading, writing, modification or deletion of those objects depending on level of access.

Access Control. The process of granting or denying specific requests to:

1. Obtain and use information and related information processing services; and

2. Enter specific physical facilities.

Access Control Point. Any physical location in a facility including designated entry/exit points where it would normally be possible for a person to pass from one area into another (for example, a door, elevator, window, stairwell, and so forth) that has been either locked or is restricted from free access by the presence of a security guard or access control device such as a card reader or biometric reader.

Access Control System. A defined method for restricting either physical or electronic access to the sensitive or confidential resources of an organization. An access control system enables an authority to control access to areas and resources in a given physical facility or information system.

Account Requester. A Forest Service employee authorized to request an account on behalf of another employee, contractor, or cooperator.

Agency Dashboard. An agency-level dashboard representation that aggregates data from a collection system and provides graphical reports and system security status to promote situational awareness.

Alternate Site. A facility that is able to support system operations in restoring critical systems to an acceptable level when the main site has been rendered unusable or unstable by a

disaster either manmade or natural as defined in the disaster recovery plan (DRP). Sites are referred to as: cold, warm, hot, mobile, and mirrored.

Annual. For the purposes of this policy and related procedures, "annual" means once per calendar year.

Application. A system that performs a clearly defined function for which there are readily identifiable security considerations and needs (such as, an electronic funds transfer system or an air traffic control system).

Application Partitioning. The separation of user functionality (including user interface services) from information system management functionality. Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate.

Application Program Manager. The official responsible for the system or application during its initial development and acquisition, and who is concerned with cost, schedule, and performance issues.

Assessment. See "Security Control Assessment."

Assessment Team. Personnel who validate the results of the risk assessment and verify that the system security plan controls are present and operating correctly. Members of the Assessment Team are independent of the IT organization and the business function responsible for developing and operating the information system. Formerly known as a Security Test and Evaluation Team.

Asset. A major application (MA), general support system (GSS), high-impact program, physical plant, mission-critical system, or logically related group of systems. Also, a physical or intangible item of value to an organization or individual.

Audit Reduction. Reduction in the amount of information contained in audit records as well as the filtering of raw log data into useful information.

Authentication. A security control or service that ensures only authenticated individuals are allowed access to information system resources by verifying the identity of a user, process, or device.

Authenticator. A device or piece of information that uniquely identifies a user of an information system. Authenticators include, but are not limited to, tokens, public key infrastructure (PKI), certificates, passwords, and key cards.

Authorization Boundary. All components of an information system to be authorized for operation by an Authorizing Official (AO) and excludes separately authorized systems to which the information system is connected.

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

Authorized Network Device. A component used to connect computers or other electronic devices within the network and has been approved for use within the system or authorization boundary.

Authorized Software. Software that is part of the standard Forest Service image, software baseline, pre-approved software list, or has received Forest Service technical approval (FSM 6610). Software baseline includes software commonly used by business units, for example, Fire, GIS, and Research, that the Forest Service owns a Forest Service license.

Authorizing Official (AO). 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. Previously known as the Accrediting Authority.

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

Background Investigation. An investigation to determine the suitability, eligibility, or qualifications of individuals for Federal employment, for work on Federal contracts, or for access to classified information or restricted information systems or functions. The level of scrutiny will differ depending on the sensitivity of the functions to be performed or the information accessed by the individual being investigated. A background investigation can include written or telephone inquiries and/or personal contacts.

Backup. Copying information system files and data to a second, separate medium, or area, such as a disk, tape, or alternate disk partition, as a precaution in case the first or primary medium fails, or data contained on the first or primary medium is damaged or lost.

Baseline Configuration. The documentation, hardware, and software that make up a configuration item (CI) at a given point in its life cycle. The baseline serves as a point of departure or reference for the next life cycle stage, and which can be changed only through

change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes. In the Forest Service standard life cycle, baselines are established after each life cycle phase.

Best Practices.

1. For purposes of IT, those techniques, or methodologies that, through experience and research, have proven to reliably lead to a desired result. A commitment to using the best practices in any field is a commitment to using all the knowledge and technology at one's disposal to ensure success.

2. In the software development process, those well-defined methods that contribute to a successful step in product development. Throughout the software industry, some best practices are widely followed; some more commonly used are an iterative development process, requirement management, quality control, and change control.

Business Impact Analysis (BIA). An analysis of the business processes and interdependencies used to characterize contingency requirements and priorities in the event of a significant disruption of service.

Chain of Custody. The identification, protection, and tracking of evidence by each responsible party to prevent loss, breakage, alteration, or unauthorized handling, by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

Change Control Board (CCB). A body of qualified individuals responsible for controlling configuration management (CM), including approval of baseline documentation and the review, analysis, and approval of configuration changes for individual information systems.

Collaborative Computing. Applications and technology (such as group video and audio conferencing) that allow two or more individuals to share information real time in an inter- or intra-enterprise environment.

Common Control. A security control that is inherited by one or more organizational information systems.

Compensating Security Controls. The Management, Operational, and Technical controls (safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the Low, Moderate, or High baselines described in NIST Special Publication (SP) 800-53, Rev. 3 that provide equivalent or comparable protection of an information system.

Computer. A general-purpose machine that processes data according to a set of instructions that are stored internally either temporarily or permanently. The computer and all

equipment attached to it are called hardware. The instructions that tell it what to do are called "software." A set of instructions that perform a particular task is called a "program" or "software program."

Computer Security Incident. Any adverse event that affects or threatens the confidentiality, integrity, or availability of some aspect of an information system or the data it contains.

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

Configuration. The functional and/or physical characteristics of a system as specified in the technical documentation and realized in a product. It includes all of the characteristics of the system that must be controlled, such as version, content, technical documentation, data needed for operation, and other essential elements.

Configuration Item. Any piece of hardware, software, or both that satisfies an end use function and is designated for separate configuration management, such as individual software applications contained by the same system.

Configuration Management (CM). Controlling and documenting the configuration of an information system throughout its life to ensure that the system components are well defined and cannot be changed without proper justification and full knowledge of the consequences.

Configuration Settings. The configurable parameters of the IT products that comprise the information system.

Configuration Settings Management (CSM). A process used to identify and control configurable parameters on all devices on the network.

Contingency Plan (CP). A plan for responding to emergencies such as attacks, disruptions, or disasters to sustain or restore systems and functions affected by the event, minimize impact, and eventually repair damage and return to normal operations. Contingency Plans normally include emergency response and backup operations. It may also point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions. See also Information System Contingency Plan (ISCP).

Contingency Planning. The dynamic development of a coordinated recovery strategy for information systems or applications, operations, and data after a significant disruption. The planning process requires several steps: develop policy; conduct BIA; identify preventive controls; develop recovery strategies; develop contingency plan; test and exercise the plan; train personnel; and maintain the plan.

Contingency Plan Testing. Either a tabletop or a functional test to validate and evaluate contingency procedures and the ability of recovery teams to implement the plan. It identifies any deficiencies in the plan that should be addressed during plan maintenance.

Continuity of Operations Plan (COOP). A plan for restoring Forest Service essential functions (often a headquarters or similar level element) at an alternate site for up to 30 days following a disaster or other event that makes the primary site unusable. Minor disruptions that do not require relocation to an alternate site are typically not addressed.

Continuous Monitoring. The process of maintaining ongoing awareness of information security, vulnerabilities, and threats in order to support organizational risk management decisions.

Control Plane Traffic. External telecommunications services that provide data and/or voice communications services. Examples of control plane traffic include Border Gateway Protocol routing, Domain Name System (DNS), and management protocols.

Controlled Unclassified Information (CUI). Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and Government-wide policies but is not classified under E.O. 13526, Classified National Security Information, or the Atomic Energy Act, 42 U.S.C. § 2011, as amended. (Source: E.O. 13556, Controlled Unclassified Information).

Corporate Data. Information owned, collected, maintained, or generated by the enterprise that has inherent value to and is intended for consistent, shared use within the enterprise. For example, a database of the enterprise's customer information would be considered corporate data. Documents generated outside the Forest Service but used by a single employee while executing assigned duties would not be considered corporate data.

Credential. A security badge, an identification card, a smart card, or other personal identity verification (PIV) device issued to each person who is allowed unescorted access into IT restricted space. A credential is an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.

Criticality Analysis. The identification of critical system components and functions considering applicable laws, executive orders, regulations, directives, policies, standards, system functionality requirements, system and component interfaces, and system and component dependencies. Criticality analysis is important for organizational systems that are designated as high value assets.

Cryptography. The study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin.

De-Identification. The process of removing the association between a set of identifying data and the data subject in order to prevent revealing personally identifiable information. [SI-19 PRIV]

Demilitarized Zone (DMZ). A network that connects an untrusted network to a trusted network but is part of neither.

Determination of Suitability. A formal, documented determination of whether or not a person is eligible for Federal work, and associated information system access, based on relevant aspects of that person's character or conduct as revealed during the course of a background investigation and screening process.

Disruption. An unplanned event, such as a power outage or facility damage, that causes an information system to be inoperable or unavailable for an unacceptable length of time.

Due Care. The minimum and customary practice of responsible protection of assets.

Due Diligence. The prudent management and execution of due care.

Emergency Account. A limited duration account granted during times of immediate, critical need, such as incident response or disaster recovery, when there is not time to follow established personnel screening and account creation procedures.

Encryption. The process of transforming readable information, such as plain text, into cipher text, a type of code that requires a secret key or password to be transformed back into the original readable information.

Endpoint Detection and Response (EDR). A form of technology that combines real-time continuous monitoring and collection of endpoint data (for example, networked computing devices such as workstations, mobile phones, servers) with rules-based automated response and analysis capabilities.

Exceptions and Exception-Specific Waivers. An official request to deviate from a specific requirement submitted to the Authorizing Official when a system owner determines that compliance with the provisions of this policy or any related information security standard would adversely impact the system or business process.

Facility Manager. The Line Officer (or staff member[s] with authority delegated by the Line Officer) who has the responsibility for managing a facility (campus, building, or space within a building) that also contains IT controlled space or IT restricted space.

Firewall. A hardware and/or software system designed to prevent unauthorized access to or from a private network, particularly unauthorized access from the Internet. A firewall typically examines all traffic to or from a private network and blocks any that does not meet specified security criteria.

Gap Analysis. A study to identify areas or issues in policies, plans, or processes that have been addressed either incompletely or not at all.

General Support System (GSS). An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and/or applications that, in turn, support mission-related functions.

Generic System Access Account. A system, functional, multi-user or non-user-based account. The account is not directly assigned to a single user for the entire life of the account.

Generic System Access Account Manager. The Forest Service employee designated as custodian of a given generic system access account. The Manager is responsible for the actions performed by those persons using said account. See Generic System Access Account.

Hardware Asset Management. A process used to identify all authorized and unauthorized devices connected to the Forest Service network.

High Value Asset. A system identified by USDA and Forest Service Management which information value, is deemed mission essential, and/or has been designated as Federal Civilian Enterprise Essential (see OMB Memorandum M-19-03 “Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program”).

Identity Proofing. The process of collecting, validating, and verifying a user’s identity information for the purposes of establishing credentials for accessing a system. Identity proofing is intended to mitigate threats to the registration of users and the establishment of their accounts.

Image. The current approved operating system and corporate software initially installed on IT devices. Images change as patches, updates, and new corporate software is installed.

Incident Handling. The mitigation of violations of security policies and recommended practices.

Incident Reporting. Notification to appropriate officials, such as Cyber Incident Response and Recovery Branch (CIRRB), that an incident is suspected, confirmed, or in progress, and ongoing communication and analysis related to the incident or its resolution.

Incident Response Plan (IRP). The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber-attack against an organization’s information system(s).

Individual. A citizen of the United States or an alien lawfully admitted for permanent residence.

Information. Forest Service data in digital or hardcopy format at any stage of processing such as, but not limited to, input, output, storage, transmission, or hardcopy.

Information Collection Request. Obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public of facts or opinions regardless of the form or format. Typical formats include, written report forms, application forms, schedules, questionnaires, reporting or recordkeeping requirements, or similar methods calling for the collection of information.

Information Exchange. Information systems that communicate with each other via hardware or network linkages for the purpose of exchanging resources, or transmitting, or providing access to data.

Information Exchange Agreement. A document specifying protection requirements and responsibilities for information being exchanged outside of system authorization boundaries. Similar to the interconnection security agreement but does not include technical details associated with an interconnection. The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (such as, government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system.

Information Exchange Security Agreement (IESA). A generic term for a class of documents that specify protection requirements and responsibilities for information being exchanged outside of the system authorization boundary. IESAs includes interconnection security agreements, information exchange agreements, memoranda of understanding or agreement (MOU/A), service level agreements, user agreements, nondisclosure agreements.

Information in Identifiable Form. Information in an IT system or online collection that directly identifies an individual (name, address, social security number, or other identifying number or code, telephone number, email address, and so forth); or by which an agency intends to identify specific individuals in conjunction with other data elements, (indirect identification). These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.

Information Owner. The official with the statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Information Sharing. Information shared with partners that may be restricted in some manner based on some formal or administrative determination. Examples of such information include, contract-sensitive information, classified information related to special access programs or compartments, privileged information, proprietary information, and personally

identifiable information. Security and privacy risk assessments as well as applicable laws, regulations, and policies can provide useful inputs to these determinations.

Information Sharing Partner. Individual, group, or organizational level that shares information content, type, security category, or special access program or compartment. Access restrictions may include non-disclosure agreements (NDA).

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Contingency Plan (ISCP). A coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data after a disruption. See also Contingency Plan (CP).

Information System Owner. See System Owner.

Information System Security Officer (ISSO). The individual responsible to the Information System Security Manager (ISSM) and to the AO or system owner for ensuring the required operational security is maintained for an information system.

Information System Security Manager (ISSM). Oversees the cybersecurity program of an information system or network, including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It also includes devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information, commonly known as the Internet of Things (IoT).

Information Technology (IT) Controlled Space. Physical locations that contain less critical IT components or any other IT components not identified as being in IT restricted space. This would include telecommunication network access points (wired or wireless routers, switches, LAN or other network patch panels, modems, or other data circuit terminating equipment) or servers and associated IT equipment. Individual cabinets, cages, lockers, lockable racks, closets, or small rooms containing such equipment (including computer training rooms), and computer rooms servicing regional or smaller audiences are examples of IT controlled space.

Information Technology (IT) Resources. Forest Service-owned, leased, managed, or authorized components of the IT infrastructure, including but not limited to personal computers and related peripheral equipment and software, library resources, telephones, cellular phones, facsimile machines, photocopiers, Internet connectivity, and access to Internet services and e-mail.

Information Technology (IT) Restricted Space. Special use space in Forest Service facilities that house web farms, computer or telecommunications equipment/devices and the general security employed surrounding these areas.

Integrity. Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity. System integrity assurance requires that a system perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Interconnection Security Agreement (ISA). A type of information exchange agreement established between the organizations that owns and operates connected IT systems to document the technical requirements of the interconnection.

Intrusion Detection. The process of monitoring the events occurring in a computer or network systems and analyzing them for signs of attempts to bypass security controls or to compromise the integrity, confidentiality, or availability of the system.

Least Privilege. The principle that an information system should enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

Life Cycle. Refer to System Development Life Cycle (SDLC).

Litigation Hold. The legal requirement to preserve all forms of relevant information created, stored, or accessed by Forest Service employees when litigation is reasonably anticipated. A Litigation Hold is initiated by a notice or communication from legal counsel to the Forest Service that suspends the normal disposition or processing of records, such as backup tape recycling, archived media and other storage and management of documents and information. A Litigation Hold will be issued as a result of current or anticipated litigation, audit, government investigation or other such matter to avoid evidence spoliation.

Logical Access. The ability to interact electronically with the data in an information system, normally through access control measures such as providing a username and password.

Major Application (MA)/Information System. An information system that requires special management attention because of its importance to the Forest Service's mission, programs, or business.

Major Change. Changes that affect the security controls of an information system and could render the system vulnerable to compromise or intrusion.

Malware/Malicious Code. A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. A virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.

Management [Security] Controls. The safeguards or countermeasures for an information system that focus on the management of risk and the management of information system security.

Marking. Application or use of human-readable security attributes.

Maximum Tolerable Downtime. The amount of time mission or business process can be disrupted without causing significant harm to the organization's mission. (Source: NIST SP 800-34 Revision 1).

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 (for example, digital media such as diskettes, tapes, removable hard drives, flash or thumb drives, compact discs, and digital video discs and non-digital media such as paper or microfilm).

Memorandum of Understanding/Agreement (MOU/A). A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission, by establishing, operating, and securing a system interconnection.

Minimal Additional Expense. In the context of employees' limited personal use of Forest Service IT resources (allowed under DR 3300-1), those situations where the Forest Service is already providing equipment or services and the employee's use of such equipment or services would not result in any additional cost to the Forest Service; involves only normal wear and tear on equipment; or would expend only small amounts of electricity, ink, toner, or paper.

Misuse. The use of any Forest Service IT resource in a way that violates Department or Forest Service policy or local, State, or Federal law.

Mobile Code. Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript.

Mobile Device. Portable cartridge/disk-based, removable storage media (for example, floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory). Portable computing and communications device with information storage capability (for example, notebook/laptop computers, personal digital assistants, cellular telephones, smart phones, tablets, digital cameras, and audio recording devices).

Monitoring. The routine process of recording activities executed on information systems for the purpose of identifying and resolving problems.

Need to Know. A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more.

Non-Disclosure Agreement (NDA). A legal contract/agreement between at least two parties which outlines confidential materials or knowledge the parties wish to share with one another for certain purposes but wish to restrict from generalized use. A contract/ agreement through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of trade secret. As such, an NDA can protect non-public business information.

Occupant Emergency Plan (OEP). A plan for how occupants of a facility will respond to a fire, attack, severe weather, medical emergency, or other event that poses a potential threat to the health and safety of personnel, the environment, or property. The OEPs are usually specific to a particular facility and its geographic location.

Ongoing Authorization. The subsequent risk determinations and risk acceptance decisions taken at agreed upon and documented frequencies in accordance with the organization's mission/business requirements and risk tolerance. An OA is an event-driven security authorization process whereby the Authorizing Official is provided with a near real-time security state of the system to determine its acceptable operational status.

Operational [Security] Controls. The safeguards or countermeasures for an information system that are primarily implemented and executed by people (as opposed to systems).

Peer-to-Peer Networking. A form of two-way Internet communication established via the use of special software, in which all machines involved act as both client and server.

Personal Identity Verification (PIV). A physical artifact (for example, identity card or "smart card") issued to an individual that contains stored identity credentials (for example, photograph, cryptographic keys, or digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

Personally Identifiable Information (PII). Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, and so forth, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, and so forth.

Personal Use. Activity conducted for purposes other than accomplishing official business or otherwise authorized activity. Employees are allowed to make limited personal use of telecommunications and IT and resources under the provisions of DR 3300-1 but are specifically prohibited from using Forest Service IT resources for uses such as maintaining or supporting a private business.

Personnel Screening. The process of reviewing the character or conduct of a person to determine if they are suitable for the proposed level of access to Forest Service information and information systems. Screening will typically involve a review of the results of a background investigation and will result in either a favorable or non-favorable judgment (adjudication) as to the suitability of the individual for the proposed level of access.

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

Preventive Measures. A risk management process implemented to identify, control, and mitigate risks or threats to an information system so as to reduce or eliminate vulnerabilities and the consequences of threats.

Pristine Media. The original, non-editable media (normally a compact disc) obtained from the manufacturer with the software license.

Privacy Impact Assessment (PIA). An analysis of how information is handled:

1. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,

2. To determine the risks and effects of collecting, maintaining, and disseminating sensitive information or information in identifiable form in an electronic information system, and

3. To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks (E-Government Act of 2002).

Privacy Officer. The Forest Service official responsible for development and implementation of policies and procedures necessary for compliance with all privacy-related

legislation and regulation, and for conducting oversight activities to ensure such compliance within the Forest Service.

Privacy Threshold Analysis (PTA). Methodology that provides information technology (IT) security professionals with a process for assessing whether a PIA is necessary.

Privilege. In the context of the policy for limited personal use provided by DR 3300-1, the extension by the Forest Service to its employees of the opportunity to use Forest Service telecommunications and IT equipment and services for limited personal use. This privilege, however, does not give employees the right to use Forest Service IT resources to modify such equipment, including loading personal software or making configuration changes.

Privileged User. A privileged user is an individual who is authorized to access system control, monitoring, or administration functions on Forest Service systems. These are:

1. "Super user," "root," or equivalent access, such as access to the control functions of the information system/network or administration of user accounts.

2. Access to change control parameters of routers, multiplexers, and other key information system/network equipment or software.

3. Authority to control and change program files, and other users' access to data.

4. Direct (unmediated) access to operating system level functions that would permit system controls to be bypassed or changed.

5. Access and authority for installing, configuring, monitoring, or troubleshooting security monitoring functions such as network/system analyzers, intrusion detection software, firewalls, or for performance of network operations.

Public Key Infrastructure (PKI). A framework for creating a secure way to exchange information over the internet based on public key cryptography. A PKI uses digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an internet transaction.

Record. Any item, collection, or grouping of information about an individual, identifiable to that individual and maintained by an agency (Privacy Act).

Recovery. Restoring a failed, damaged, or disrupted information system to a previous known good state. Recovery normally relies on the use of system backups.

Recovery Point Objective. The point in time in which data must be restored/recovered in order to resume processing and meet full business objectives.

Recovery Time Objective. The overall length of time an information system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business functions.

Remediation. The process of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application.

Remote Access. The ability to connect and log into a network from an offsite location such as a home, satellite office, hotel room, or airport usually by means of a direct connection such as dialup or through the public Internet using secure connection software.

Residual Risk. The risk that remains after security measures have been applied.

Risk. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

1. The adverse impacts that would arise if the circumstance or event occurs; and

2. The likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and consider the adverse impacts to organizational operations and assets, individuals, other organizations, and the Nation.

Risk Assessment (RA). The process of identifying the risks to system security by determining applicable threats, vulnerabilities, the probability of a vulnerability being exploited, and the resulting impact to the system and the business function it supports.

Risk Assessment Team. An ad hoc team of information resource management specialists that includes a team manager, a systems engineer, and a network specialist. The team schedules and performs in depth RAs of Forest Service information systems and recommends options for mitigating risk findings.

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

Risk Management Framework (RMF). The NIST-developed organizational approach to the management of risk. The RMF entails:

1. Building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls.

2. Maintaining awareness of the security state of information systems on an ongoing basis through enhanced monitoring processes; and

3. Providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.

Role-Based Training. The targeted teaching of concepts and skills based on a person's role in an organization or operation and the specific functions they perform.

Roles and Responsibilities. The functions performed by a position in a specific situation and obligations to tasks or duties for which that position is accountable.

Rules of Behavior. A set of rules that clearly delineate responsibilities and the expected behavior of all individuals with regard to access to Forest Service information and information system usage.

Security Assessment. See Security Control Assessment.

Security Awareness. A learning process that demonstrates to end users the importance of IT security.

Security Capability. A set of related security controls to achieve a common purpose.

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 Forest Service operations, assets, or individuals.

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

Security Controls. Management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Test and Evaluation (ST&E). An evaluation of all hardware, software, and physical security features that are part of an information system to determine what threats and

vulnerabilities exist. The findings are documented, and recommendations are made that may be included in the Risk Assessment (RA).

Security Training. The teaching of system security skills so that a specific function can be performed without creating unacceptable information system security risks.

Senior Agency Officer for Privacy (SAOP). Senior Forest Service official with overall Forest Service-wide responsibility for information privacy issues.

Senior Information Collection Officer (SICO). The focal point for all Department-wide matters relating to information collection, privacy, paperwork reduction, and elimination. The SICO designates individuals to serve as Information Collection Officers who serve as points of contact on information collection request matters

Sensitive Information. Any information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Separation of Duties. The principle of distributing critical information system support and processing functions among different individuals or positions to ensure that no one person or position has all authority or access necessary to conduct fraudulent activity or compromise information security controls.

Server. Equipment that enables the sharing of data or services across a network.

Service Level Agreement (SLA). A formal negotiated agreement between two parties. It is a contract that exists between customers and their service provider, or between service providers. It records the common understanding about services, priorities, responsibilities, guarantees, etc. with the main purpose to agree on the level of service. For example, it may specify the levels of availability, serviceability, performance, operation, or other attributes of the service, for example, billing, and even penalties in the case of violation of the SLA.

Significant Change. A modification that impacts the operating environment, functional design, operation, or protective controls required for a system. Changes in user audiences, owning organization, public access, and communication methods are considered significant changes. Other examples of a significant change include, but are not limited to: a change in criticality and/or sensitivity level that causes a change in the countermeasures required; a change in the security policy; a change in the threat of system risk; a change in the activity that requires a different mode of operation; additions or a change to the operating system or to software providing security features; additions or a change to the hardware that requires a change in the approved security countermeasures; a breach of security, a breach of system

integrity, or an unusual situation that appears to constitute a breach, a significant change to the physical structure of the facility or to the operating procedures, and a significant change to the configuration of the system.

Software Asset Management. A process used to identify authorized and unauthorized software on all network attached devices.

Spam. Unsolicited commercial e-mail; the copying, transmission, or retransmission of chain letters; or other unauthorized mass mailings (for example, sending information to lists of multiple unknown recipients where no official business relationship exists).

Sponsor. The official who acts on behalf of the Forest Service to request credentials and access permissions for an associate/affiliate. Responsibilities include coordinating data gathering and entry into USDA Person Model with the associate/affiliate, initiating the background investigation, and authorizing the associate/affiliate for a LincPass. Depending on the applicant's employment status, a Sponsor may be a Contracting Officer, Contracting Officer's Representative (COR), Procurement and Property Services (PPS) Contracting Officer, Grants Management Specialist, or other Forest Service official.

Supply Chain. Linked set of resources and processes between and among multiple levels of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their life cycle

Supply Chain Risk Management (SCRM). The process of identifying, assessing, and mitigating the risks to the integrity, trustworthiness, and authenticity of products and services within the supply chain of a system.

Supply Chain Risk Management Plan. A plan that provides SCRM policy implementation, requirements, constraints, and implications. It addresses managing, implementation, and monitoring of SCRM controls and the development and sustainment of a system across the SDLC to support mission and business functions. It describes the SCRM controls appropriate for the information to be transmitted, processed, or stored by the system.

System. A logical set of IT processes, communications, storage, and related resources. The elements within these boundaries constitute a single system.

System Administrator. A privileged user who manages the computer systems in an organization. A system administrator is involved with OS, hardware installations, and configurations and may be involved with application installations and upgrades. Responsibilities may include installing new applications, distributing software upgrades, monitoring daily activity, enforcing licensing agreements, developing a storage management program, and providing for routine backups.

System Component. Information system components include, for example, mainframes, workstations, servers (for example, database, electronic mail, authentication, web, proxy, file, domain name), network components (for example, firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications

System Development Life Cycle (SDLC). The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal, which instigates another system initiation.

System Maintenance. The modification or upkeep of information system hardware and software to sustain or improve performance, to correct faults or deficiencies, or to adapt the system to changes in environment or requirements. Maintenance can be performed on-site or remotely, and normally involves activities such as testing, cleaning, or adjusting of equipment, applying system updates or changes, or reorganizing stored data to improve performance.

System of Records. A group of records under the control of any agency where information is retrieved by the name of the individual, by some identifying number or symbol, or by other identifiers assigned to the individual.

System of Records Notice (SORN). Details about systems containing information cited in the Privacy Act must be published in the Federal Register as a Records Notice, specifying to the public what information is contained in the system, how it is used, and how an individual may gain access to their information.

System Owner. Officials having responsibility for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.

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. The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

Technical [Security] Controls. The safeguards or countermeasures for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Threat. A circumstance, condition, or event with the potential to cause harm to personnel or network resources in the form of destruction, disclosure, modification of data, denial of service, or fraud, waste, and abuse. The most common security threats are to network systems, including impersonation, eavesdropping, and denial of service, identity theft, and packet replay/modification.

Token. Something that the Claimant possesses and controls (typically a key or password) that is used to authenticate the Claimant's identity (SP 800-63). Tokens are often used in conjunction with passwords to create more secure two-factor authentication.

Trust Anchor.

Two-factor Authentication. Describes an electronic identity verification process that requires the use of at least two of the three authentication factors recognized by NIST SP 800-63, Electronic Authentication Guideline:

1. Something known (for example, a password).

2. Something you possess (for example, an identification (ID) badge or a cryptographic key); or

3. Something that identifies who you are (for example, a voice print or other biometric).

Unauthorized Software. Any executable code that is not part of the standard Forest Service image or has not received Forest Service TA and is not appropriately licensed.

User. Individual or (system) process authorized to access an information system.

Virtual Private Network (VPN). A virtual network built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

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

Vulnerability Management. Identifying vulnerabilities classified by risk level and ideally remediated in the Forest Service environment.

Zero Trust Architecture (ZTA).

security model eliminates implicit trust in any one element, component, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses

6680.05a - Abbreviations and Acronyms

Exhibit 01 contains a list of the abbreviations and acronyms used in this chapter.

6680.05a - Exhibit 01

List of Abbreviations and Acronyms

Abbreviations and Acronyms	Term
A&A	Assessment and Authorization
ACIO	Assistant Chief Information Officer
ACISO	Assistant Chief Information Security Officer
AO	Authorizing Official
ATO	Authority to Operate
BCP	Business Continuity Plan
BIA	Business Impact Analysis
C2	Controlled Access Protection (security rating)
CCB	Change Control Board
CFR	Code of Federal Regulations
CIRRB	Cybersecurity Incident Response and Recovery Branch
CISO	Chief Information Security Officer
CM	Configuration Management
CMP	Configuration Management Plan
CO	Contracting Officer
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan
COR	Contracting Officer’s Representative
CP	Contingency Plan
CPC	Contingency Planning Coordinator

Abbreviations and Acronyms	Term
CPIC	Capital Planning and Investment Control
CSAM	Cyber Security Assessment and Management
CSM	Configuration Settings Management
CUI	Controlled Unclassified Information
DM	Departmental Manual
DMZ	Demilitarized Zone
DNS	Domain Name System
DPM	Department Personnel Manual
DR	Departmental Regulation
DRP	Disaster Recovery Plan
EA	Enterprise Architecture
EDR	Endpoint Response and Detection
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FS	Forest Service
FSH	Forest Service Handbook
FSM	Forest Service Manual
FY	Fiscal Year
GSS	General Support System
HRM	Human Resource Management
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HVA	High Value Asset
HVAC	Heating, Ventilation, Air Conditioning
ID	Identification
IoT	Internet of Things

Abbreviations and Acronyms	Term
IP	Internet Protocol
IRP	Incident Response Plan
IS	Information System
IESA	Information Exchange Security Agreement
ISCP	Information Security Contingency Plan
ISCM	Information Security Continuous Monitoring
ISA	Information Security Agreement
ISSO	Information System Security Officer
ISSM	Information System Security Manager
IT	Information Technology
LAN	Local Area Network
LEI	Law Enforcement and Investigations
MA	Major Application
MOU/A	Memorandum of Understanding/Agreement
NARA	National Archives and Records Administration
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology
NRE	Natural Resources and Environment
OCIO	Office of the Chief Information Officer
OEP	Occupant Emergency Plan
OIG	Office of the Inspector General
OMB	Office of Management and Budget
ORMS	Office of Records and Management Services
OS	Operating System
POA&M	Plan of Action and Milestones
PDA	Personal Digital Assistants
PIA	Privacy Impact Assessment

Abbreviations and Acronyms	Term
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PPS	Procurement and Property Services Staff
PKI	Public Key Infrastructure
PM	Program Management
POC	Point of Contact
PRIV	Privacy Control
PTA	Privacy Threshold Analysis
RA	Risk Assessment
RBD	Risk-Based Decision
RFC	Request for Comment
RMF	Risk Management Framework
SAOP	Senior Agency Official for Privacy
SBU	Sensitive but Unclassified
SCRA	Supply Chain Risk Assessment
SCRM	Supply Chain Risk Management
SCRMP	Supply Chain Risk Management Plan
SDLC	System Development Life Cycle
SIA	Security Impact Analysis
SICO	Senior Information Collection Officer
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SORN	System of Records Notice
SP	Special Publications
SQL	Structured Query Language
SSP	System Security Plan
ST&E	Security Test and Evaluation

Abbreviations and Acronyms	Term
TLS	Transport Layer Security
U.S.C.	United States Code
USDA	United States Department of Agriculture
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
ZTA	Zero Trust Architecture

6680.06 - References

1. *Carnegie-Mellon, Capability Maturity Model Integration Institute.* Provides standards for configuration management (CM).

2. *Telework Enhancement Act of 2010*. Requires each executive agency to establish a policy under which eligible employees of the Agency may be authorized to telework.

6680.06a - National Institute of Standards and Technology Special Publications

National Institute of Standards and Technology (NIST) Special Publications (SPs) are listed in exhibit 01 and are available electronically from *Computer Security Resource Center*.

6680.06a - Exhibit 01

Applicable National Institute of Standards and Technology Special Publications

Publication Number	Date	Title	Description
NIST SP 800-12 Rev. 1	June 2017	An Introduction to Computer Security	Provides a broad overview of computer security to help readers understand their computer security needs and develop a sound approach to the selection of appropriate security controls.
NIST SP 800-16	April 1998	Information Technology Security Training Requirements: A Role- and Performance-Based Model	Presents a tactical level, conceptual framework for providing role-based IT security training.
NIST SP 800-18, Revision 1	February 2006	Guide for Developing Security Plans for Federal Information Systems	Provides an overview of the security requirements of an information system; describes controls for meeting those requirements, and outlines security awareness and training program elements.
NIST SP 800-30, Revision 1	September 2012	Guide for Conducting Risk Assessments	Provides guidance for conducting risk assessments of federal information systems and organizations.

Publication Number	Date	Title	Description
NIST SP 800-35	October 2003	Guide to Information Technology Security Services	Provides guidelines for developing agreements that define the service levels for the service provides within a security services life cycle.
NIST SP 800-37, Rev. 2	December 2018	Risk Management Framework for Federal Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy	Provides guidelines applying the Risk Management Framework to Federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

Publication Number	Date	Title	Description
NIST SP 800-39	March 2011	Managing Information Security Risk: Organization, Mission, and Information System View	Provides guidance for an integrated, organization-wide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of federal information systems.
NIST SP 800-40, Version 4	April 2022	Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology	This document is to help organizations improve their enterprise patch management planning so that they can strengthen their management of risk.
NIST SP 800-41, Rev. 1	September 2009	Guidelines for Firewalls and Firewall Policy	Provides guidance on the design, selection, deployment, and management of firewalls and firewall environments.

Publication Number	Date	Title	Description
NIST SP 800-47, Rev. 1	July 2021	Managing the Security of Information Exchanges	Provides guidance to define the scope of information exchange, describe the benefits of securely managing information exchange, identify types of information exchanges, discuss potential security risks associated with information exchange, and detail a four-phase methodology to securely manage information exchange between systems and organizations.
NIST SP 800-50	October 2003	Building an Information Technology Security Awareness and Training Program	Guidance for building and maintaining a comprehensive awareness and training program, as part of a Forest Service IT security program.

Publication Number	Date	Title	Description
NIST SP 800-53, Rev. 5	December 2020	Security and Privacy Controls for Federal Information Systems and Organizations	Provides a catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation from a diverse set of threats including hostile cyber-attacks, natural disasters,).
NIST SP 800-53A, Rev. 5	January 2022	Assessing Security and Privacy Controls in Information Systems and Organizations	Provides guidelines for developing security assessment plans and associated security control assessment procedures that are consistent with NIST SP 800-53, Rev. 5.

Publication Number	Date	Title	Description
NIST SP 800-53B	December 2020	Control Baselines for Information Systems and Organizations	Provides security and privacy control baselines for the Federal Government.
NIST SP 800-58	January 2005	Security Considerations for Voice Over IP (VoIP) Systems	Guidance for establishing secure VoIP networks.
NIST SP 800-60, Rev. 1	August 2008	Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide, Volume 2: Appendices	Identifies information types and information systems and assigns impact levels for confidentiality, integrity, and availability.
NIST SP 800-61, Rev. 2	August 2012	Computer Security Incident Handling Guide	Provides guidance on organizing a computer security incident response capability and handling incidents.
NIST SP 800-63-3	March 2020	Digital Identity Guidelines	Guidance for allowing individuals to remotely authenticate to a Federal IT System.
NIST SP 800-70, Rev. 4	February 2018	National Checklist Program for IT Products—Guidelines for Checklist Users and Developers	Provides an overview of the NIST checklist program and explains how to retrieve security configuration checklists from the NIST repository.

Publication Number	Date	Title	Description
NIST SP 800-72	November 2004	Guidelines on Personal Digital Assistant (PDA) Forensics	Provides an in-depth look into PDAs and explains the technologies involved and their relationship to forensic procedures. Discusses procedures for the preservation, acquisition, examination, analysis, and reporting of digital information present on PDAs, as well as available forensic software tools that support those activities.
NIST SP 800-73-4	February 2016	Interfaces for Personal Identity Verification	Specifies the PIV data model, Application Programming Interface, and card interface requirements necessary to comply with the mandated use cases. See FIPS Publication 201, section 6 where the interoperability across deployments or agencies is described.

Publication Number	Date	Title	Description
NIST SP 800-81-2	September 2013	Secure Domain Name System (DNS) Deployment Guide	Provides guidance on deployment guidelines for securing DNS within an enterprise.
NIST SP 800-83 Rev. 1	July 2013	Guide to Malware Incident Prevention and Handling for Desktops and Laptops	Provides an understanding of the threats posed by malware and mitigate the risks associated with malware incidents. Provides practical, real-world guidance on preventing malware incidents and responding to malware incidents in an effective, efficient manner.
NIST SP 800-84	September 2006	Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities	Provides guidance on test, training, and exercise programs for IT plans and capabilities.
NIST SP 800-86	September 2006	Guide to Integrating Forensic Techniques into Incident Response	Describes the processes for performing effective forensics activities and provides advice regarding different data sources, including files, operating systems (OS), network traffic, and applications.

Publication Number	Date	Title	Description
NIST SP 800-88 Rev. 1	December 2014	Guidelines for Media Sanitization	This guide is intended to assist Forest Service and ISOs decisions based on the level of sensitivity of their information. It does not, and cannot, specifically address all known types of media.
NIST SP 800-92	September 2006	Guide to Computer Security Log Management	Provides guidance on computer security log management.
NIST SP 800-95	August 2007	Guide to Secure Web Services	Guidance on integrating information security practices into Service Oriented Architecture (SOA) design and development based on Web services and on current and emerging standards applicable to Web services, as well as background information on the most common security threats to SOAs based on Web services.

Publication Number	Date	Title	Description
NIST SP 800-96	December 2006	PIV Card/Reader Interoperability Guidelines	Presents recommendations for PIV card readers in the area of performance and communications characteristics to foster interoperability.
NIST SP 800-100	March 2007	Information Security Handbook: A Guide for Managers	Informs members of the information Security Management Team about various aspects of information security that they will be expected to implement and oversee in their respective organizations. Provides guidance for facilitating a more consistent approach to information security programs across the Federal Government.
NIST SP 800-115	September 2008	Technical Guide to Information Security Testing and Assessment	Provides basic technical aspects of conducting information security assessments while presenting technical testing and examination methods and techniques that an organization might use as part of an assessment.

Publication Number	Date	Title	Description
NIST SP 800-122	April 2010	Guide to Protecting the Confidentially of Personally Identifiable Information (PII)	Guidance on protecting the confidentiality of a specific category of data commonly known as PII. Including context-based guidance for identifying PII and determining what level of protection is appropriate for each instance.
NIST SP 800-128	October 2019	Guide for Security-Focused Configuration Management of Information Systems	Identifies the major phases of security configuration management and describes the process of applying security configuration management practices for information systems.
NIST SP 800-137	September 2011	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations	Provides organizations with the guidance for implementing an ISCM process to specifically address assessment and analysis of security control effectiveness and organizational security status.

Publication Number	Date	Title	Description
NIST SP 800-161, Rev. 1	May 2022	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	Provides guidance to organizations on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of their organizations.

6680.06b - National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publications

National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publications are listed in exhibit 01 and are available electronically from *https://csrc.nist.gov/publications/fips*.

6680.06b - Exhibit 01

National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publications

Publication Number	Date	Title	Description
FIPS 199	February 2004	Standards for Security Categorization of Federal Information and Information Systems	Sets standards for categorizing information and information systems with the objective of providing appropriate levels of information security according to a range of risk levels.
FIPS 200	March 2006	Minimum Security Requirements for Federal Information and Information Systems	Mandates use of NIST SP 800-53.
FIPS 201-2	September 2013	Personal Identity Verification of Federal Employees and Contractors	Provides standards and procedures for proofing identities.

6681 - Security Program Management

6681.01 - Authority [Reserved]

6681.02 - Objective [Reserved]

6681.03 - Policy [Reserved]

6681.04 - Responsibility [Reserved]

6681.05 - Definitions [Reserved]

6682 - Security Management Controls

6682.01 - Authority [Reserved]

6682.02 - Objective

Implement security controls focused on the management of information security risk and to ensure, in a continuous manner, that these controls are in place, operating as intended, and providing the required level of protection for information technology (IT) resources that support the Forest Service mission.

6682.03 - Policy [Reserved]

6682.04 - Responsibility

6682.04a - Assistant Chief Information Officer for Natural Resources and Environment

The Assistant Chief Information Officer (ACIO) for Natural Resources and Environment (NRE) is responsible for:

1. Managing risk related to Forest Service information systems, including:

    a. Ensuring that there is a formal documented continuous assessment and authorization (A&A) policy.

    b. Establishing an enterprise Risk Assessment (RA) and Supply Chain Risk Assessment (SCRA) program and ensuring adequate resources are allocated for the continuing assessment and mitigation of information security risks.

    c. Ensuring information technology (IT) professionals understand their role in the RA and SCRA process, with special emphasis on the roles of system owners, developers, information system security officers, and system administrators.

d. Selecting and managing an appropriate system development life cycle (SDLC) for each information system.

e. Ensuring that the status of all weaknesses at the program-level and system-level is submitted to a higher authority each quarter.

f. Using a formal system SDLC and configuration management (CM) approach in the management of information systems in support of the risk assessment program.

g. Developing and submitting IT budgets, funding requests and business cases to implement necessary risk mitigations on Forest Service systems, as required.

2. Security planning for Forest Service information systems, including:

    a. Ensuring that all Forest Service IT General Support Systems (GSSs) and major applications (MA) are assessed and authorized and reporting status of security assessment and authorization to USDA Cyber Security as required.

    b. Ensuring that the Capital Planning and Investment Control (CPIC) process supports the determination, documentation, and allocation of the resources necessary to adequately protect information systems.

3. Ensuring that appropriate SDLCs are selected and used for all Forest Service information systems.

4. Ensuring that security requirements and controls are integrated into the SDLC from inception.

5. Ensuring that an Authorizing Official (AO) is formally appointed for each Forest Service GSS and MA, and that the AO fully accepts the responsibility for system risk and operation.

6. Ensuring that any system that has significant deficiencies identified as a result of assessment activities, audits, concurrence reviews, or other authorized processes is placed under significant management attention with limited authorization to operate (ATO) and the AO is notified of the increased risk to the Forest Service.

7. Ensuring that systems operating under an ATO undergo security assessment and authorization before the ATO expires.

8. Ensuring that final A&A packages are accurate and complete.

9. Ensuring that any system risks and security deficiencies discovered during the continuous A&A process are resolved or mitigated by appropriate security controls.

10. Ensuring that all system changes are examined to determine if new or increased security risks have been created that would require a new security assessment and authorization of the system and, if so, initiating such action.

11. Ensuring that each Forest Service General Support System (GSS) and major application (MA) continuously monitors the status of security controls and routinely performs continuous A&A according to the requirements in the current USDA Risk Management Framework (RMF) guidelines and other current Federal, Departmental, and Forest Service regulations.

12. Authorizing, chartering, and chairing (or designating a chair for) a Forest Service-level Change Control Board (CCB) and ensuring security and privacy representatives are members of CCB.

13. Ensuring that a Forest Service-wide configuration management program is implemented in accordance with FSM 6682.6, and the status of configuration management requirements are reported to USDA as requested.

14. Ensuring that sufficient training is provided to allow those responsible for configuration management to understand their roles and perform their assigned duties.

15. Formally designating a Forest Service Privacy Officer to oversee all privacy-related information security issues.

16. Ensuring that Privacy Threshold Analysis (PTA), applicable Privacy Impact Assessments (PIAs) and System of Records Notice (SORN) are conducted and submitted to appropriate authorities in accordance with USDA, Office of Management and Budget (OMB), and Forest Service policy (including the privacy provisions of Section 208 of the E-Government Act and of the Privacy Act of 1974).

17. Acting as the Senior Agency Officer for Privacy (SAOP) with the overall responsibility and accountability for ensuring the Agency's implementation of information privacy protections, including the Agency's full compliance with federal laws, regulations, and policies relating to information privacy, such as the Privacy Act. The SAOP will also have a central policy-making role in the development and evaluation of legislative, regulatory and other policy proposals which implicate information privacy issues, including those relating to the Agency's collection, use, sharing, and disclosure of personal information.

18. Ensuring compliance with requirements for immediate and long-term training needs in support of privacy requirements.

19. Ensuring compliance with requirements for protecting the confidentiality and integrity of personally identifiable information (PII).

20. Ensuring that the centralized inventory is reviewed within the organization-defined timeframe.

21. Sponsoring and promoting the continuous monitoring program within the Forest Service.

6682.04b - Assistant Chief Information Security Officer for Natural Resources and Environment

The Assistant Chief Information Security Officer (ACISO) for Natural Resources and Environment (NRE) is responsible for:

1. Supporting the Forest Service Risk Management Program by taking the following actions as required:

    a. Participating in the development of cost estimates and submissions of funding requests for mitigations.

    b. Developing and implementing Forest Service-wide policies and procedures for assessing information security risks.

    c. Ensuring that Federal Information Security Management Act (FISMA) reports reflect risk assessments performed for information systems and that each FISMA Plan of Action and Milestones (POA&M) includes action items to mitigate security weaknesses discovered through the risk assessment process.

2. Implementing an Agency-wide security and privacy assessment and authorization process in accordance with FSM 6682.4 and assisting with security and privacy assessment and authorization activities.

3. Reporting security assessment and authorization progress to the Authorizing Official.

4. Disseminating this policy to all IT professionals, Security Officers, and system owners who will be involved in the security and privacy assessment and authorization process to ensure they understand and can fulfill their roles and responsibilities.

5. Ensuring that all corrective actions are tracked and reported to USDA Cybersecurity through the POA&M process, as required.

6. Developing Forest Service-wide information security metrics and measures of performance.

7. Providing leadership to and oversight of the Information Systems Security Manager (ISSM) role.

6682.04c - Information System Security Manager

Information System Security Managers are responsible for:

1. Supporting the Forest Service Risk Management Program by taking the following actions as required:

    a. Participating in system risk and supply chain risk assessments and documentation.

    b. Verifying risk and supply chain risk assessments are conducted.

    c. Developing and implementing Forest Service-wide policies and procedures for assessing information security risks.

    d. Verifying that all IT systems undergo security and privacy assessment and authorization as required as a part of the continuous assessment and authorization (A&A) process or whenever there is a significant change to the IT system.

    e. Ensuring that system security plans (SSPs) are updated on an annual basis or when a significant change occurs to an information system to include the latest risk assessment date, major findings, mitigations, and timeframes for action.

    f. Ensuring that Federal Information Security Management Act (FISMA) reports reflect risk assessments performed for information systems and that each FISMA Plan of Action and Milestones (POA&M) includes action items to mitigate security weaknesses discovered through the risk assessment process.

2. Supporting the Forest Service system security plan by:

    a. Ensuring that the security plans for all GSS and major applications are prepared and updated in conjunction with the application's business owner, program manager, or developer.

    b. Verifying that all system security plans are submitted to the ACIO and AO.

c. Developing and maintaining an inventory of all information systems, software, and privacy; determining data sensitivity and identifying GSSs and applications, following direction in USDA DM 3575-001.

3. Ensuring that each Forest Service information system has an assigned Information System Security Officer (ISSO).

4. Ensuring that existing or legacy Forest Service information systems have cost-effective security and privacy controls in place appropriate to their stage in the system life cycle.

5. Implementing an agency-wide security and privacy assessment and authorization process in accordance with FSM 6682.4 and assisting with security and privacy assessment and authorization activities and privacy role.

6. Supporting and participating in security assessment team activities, providing guidance, testing security controls, and assisting in preparation of the final security authorization package, as required.

7. Monitoring and tracking security assessment and authorization activities using POA&Ms.

8. Supporting and facilitating the work of security and privacy assessment teams to ensure that Forest Service information systems are assessed and authorized.

9. Ensuring that all corrective actions are tracked and reported to USDA Cybersecurity through the POA&M process, as required.

10. Ensuring that all IT security program-level and system-level POA&Ms are developed, processed, disseminated, and reported as specified by the Office of Management and Budget.

11. Ensuring that risk determination is conducted as required by system owners as part of the Risk Assessment (RA) updating process, including RA updates as part of PIA updates.

12. Review and report adherence to the security control requirements related to necessary encryption, two-factor authentication, and remote access standards.

13. Reviewing adherence to security and privacy control requirements related to protecting the confidentiality and integrity of personally identifiable information (PII) privacy officer.

14. Developing and maintaining the Forest Service Assessment & Authorization Process.

6682.04d - Authorizing Official

The Authorizing Official (AO) is responsible for:

1. Approving the operation of an information system and ensuring that it is operating at an acceptable level of risk to the Forest Service.

2. Formally designating individuals responsible for security assessment, authorization activities, and the information system owner. The AO shall not delegate the security authorization decision and signing of the associated security authorization decision letter.

3. Granting or denying permission for information systems, based on acceptability of determined risk, to begin or continue operation in their intended environment through an authorization to operate (ATO).

4. Ensuring that information systems that will be used to conduct or host information collected from the public require security controls commensurate with the appropriate FISMA compliance level(s), even if PII is not collected by an information collection, and are properly authorized prior to such collection, even if Forest Service has obtained OMB clearance for the collection.

5. Approving security and privacy requirements, deviations from security policies (as agreed with the Contracting Officer (CO) and Forest Service Assistant Chief Information Security Officer) and memoranda of agreement or understanding.

6. Reviewing and approving or denying all risk-based decisions (RBDs) for all systems over which they have management authority.

7. Ensuring the implementation of USDA Information and Communication Technology Supply Chain Risk Management (ICT SCRM) strategy and approving mitigation plans for SCRM residual risks for systems within their purview in accordance with USDA DN 3540-004 or other USDA guidance.

8. Evaluating risk and supply chain risk assessment results as they become available and incorporating those results into the Forest Service decision-making process.

9. Implementing risk mitigation strategies or formally accepting residual risk through a documented RBD.

10. Resolving or addressing information system security deficiencies within 1 calendar year after discovery.

11. Reporting mitigation results to the Forest Service Assistant Chief Information Security Officer.

12. Developing and implementing configuration management plans for all systems they develop and maintain.

13. Designating the Information System Security Officer (ISSO) for their system.

6682.04e - System Owners

The system owner is responsible for the following for each of their assigned systems:

1. Incorporating security and privacy requirements and controls into the SDLC.

2. Developing, implementing, and maintaining a system security plan (SSP) for each of their information systems with guidance found in NIST SP 800-18 Rev. 1 and FSM 6680.

3. Providing Forest Service Contracting Officers (CO)s and grants management specialists applicable security requirements in accordance with applicable laws, Executive orders, directives, policies, regulations, standards, and guidance, as described in the SSP, to be included in procurement documents (such as, requests for proposals) for information systems and services.

4. Minimizing risk to the Forest Service IT infrastructure, including personally identifiable information (PII) and corporate data in the development, testing, and maintenance of the system and applications.

5. Selecting a security control baseline and tailoring the selected controls to the system.

6. Reviewing and validating security controls to ensure they are operating as intended.

7. Ensuring that system changes are made only through the change control process established for their systems.

8. Ensuring that security assessment and authorization activities of their systems are conducted in accordance with the current USDA Risk Management Framework (RMF) guidelines and NIST SP 800-37 Rev. 2.

9. Operating, maintaining, and disposing of their systems in accordance with the security plans and other documented security control requirements.

10. Coordinating and supporting security assessment and authorization for their systems, including reviewing the security authorization package before it is presented to ACIO.

11. Providing sufficient resources to:

a. Remediate system vulnerabilities discovered during security and privacy assessment activities, audits, concurrence reviews, IV&V activities, or other authorized activities.

b. Report, as required, remediation activities in the designated departmental or Forest Service designated repository used for FISMA reporting purposes.

c. Enable and ensure that system users and security support personnel obtain required role-based security and privacy training.

d. Comply with requirements to protect the confidentiality of any personally identifiable information (PII) collected and/or retained by their system.

12. Developing and maintaining configuration management (CM) plans for their systems.

13. Identifying changes to information systems that require reauthorization, in conjunction with the system Change Control Board (CCB).

14. Reviewing proposed system configuration changes for potential security and privacy impacts.

15. Ensuring that any system changes are approved and released in accordance with FSM 6682.6 and that changes that have not been approved in accordance with FSM 6682.6 are not released.

16. Managing and documenting the configuration of their systems, throughout their lifecycles, in accordance with FSM 6682.6.

17. Ensuring that authorized software products, including updates and modifications, are created from the software baseline library and controlling product releases in accordance with the system CM plan.

18. Identifying, controlling, and making selected system components or products available for review or audit.

19. Determining the system's security categorization level using the guidance in NIST SP 800-60 Rev. 1 and other applicable guidelines.

20. Ensuring that the system is scanned for vulnerabilities using appropriate tools and techniques.

21. Ensuring that all system-level POA&Ms are prepared and updated in accordance with FSM 6682.4c.

22. Ensuring that all IT security and privacy controls in the information systems are monitored on an ongoing basis.

23. Ensuring that the effectiveness and adequacy of system controls are in accordance with NIST SPs 800-37 Rev. 2 and 800-53A.

24. Ensuring that security authorization packages are updated and maintained for each information system under their responsibility, which includes documentation of the business associations and dependencies of their information system.

25. Ensuring that any information system changes are prompted through the CM and change control processes, and are updated in the information system's SSP.

26. Reviewing and approving POA&M milestones in the designated repository before final POA&M approval.

27. Addressing the requirements for connectivity with the other information systems and working to identify the security and privacy requirements if the system will be connected to other internal or external information systems, through:

    a. Monitoring security control compliance.

    b. Following NIST SP 800-47 Rev. 1 guidance on information exchange agreement and USDA DM 3575-001, Table 1, guidance on interconnection security agreements (ISA).

28. Developing and implementing the rules of behavior for appropriate use and protection of the subject data and information, including data and information shared with others, restrictions on use of social media, social networking sites, external sites/applications, posting Forest Service information on public websites, and use of email addresses and passwords for creating accounts on external sites.

29. Participating in PTA, PIA, and SORN activities.

30. Ensuring that adequate documentation for the life cycle of the information systems is produced and distributed to authorized personnel, updated when there are changes to the system, and protected in accordance with FSM 6682.7.

31. Ensuring that security controls are implemented at each phase of the system development life cycle (SDLC), and that those systems do not move to the next phase until security requirements of the current phase are met.

32. Ensuring documentation is available from vendors/manufacturers.

33. Ensuring that adequate information system documentation is available at alternate information system operating sites.

34. Continuously monitoring the effectiveness and adequacy of system controls against their baseline security requirements.

35. Designating a Risk Assessment (RA) and Supply Chain Risk Assessment (SCRA) team.

36. Ensuring that the RA and SCRA for the information system is updated whenever one of the following criteria is met:

    a. As required, as a part of the IT system's continuous monitoring of security and privacy controls, or as needed; or

    b. Updated, reflecting a configuration change to the IT system, following the Agency's change request and Configuration Management (CM) process.

37. Managing risk related to Forest Service information systems, including:

    a. Formally documenting residual risk in a residual risk statement and ensuring that threats are remediated, or that the authorizing official (AO) continues to accept these risks.

    b. Requesting formal waivers as a risk-based decision (RBD), authorized by the respective AO for information systems that do not comply with FSM 6680.

38. Ensuring that all vulnerabilities that are reported in the designated departmental or Forest Service Federal Information Security Management Act (FISMA), Plan of Action and Milestones (POA&M) repository are timely and effectively remediated.

39. Ensuring that tasks and milestones associated with remediation of system vulnerabilities are correctly and timely reported in the designated departmental or Forest Service FISMA POA&M repository.

40. Ensuring for non-archived holdings of all personally identifiable information, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete, and reducing them to the minimum necessary for the proper performance of a documented agency function.

41. Ensuring that no official files on individuals are retrieved by name or other personal identifier without first ensuring that a notice of the system of records has been published in the Federal Register.

42. Ensuring that all personnel who either have access to the system of records or who develop or supervise procedures for handling records in the system of records are

aware of their responsibilities for protecting personal information being collected and maintained.

43. Coordinating information collection request activities (surveys, forms, and so forth) with the Privacy Act Officer when developing a new or extending/revising an existing information collection request(s) and ensuring that the information collection is necessary for the proper performance of the Agency's function and has practical utility. Preparing and publishing the 60-day Federal Register notice prior to the expiration date of an existing information collection request, or the use date of a new information collection.

44. Ensuring that information system configuration changes are properly approved, controlled, and documented in accordance with FSM 6682, and that changes do not harm system security properties.

45. Ensuring that the current status of required configuration management activities is available and identifying information systems not in compliance with the requirements of FSM 6682.

46. Ensuring that only approved hardware and software is used within Forest Service system boundaries.

47. Ensuring that all requests for connections to non-Forest Service information systems are documented in the information exchange Agreement /Memorandum of Understanding (MOU), reviewed, and assessed, and that IT security and privacy recommendations are made to the System Owner, AO, and the ACIO. Terminating the agreement when no longer needed.

48. Ensuring that information systems have a documented system development life cycle, and that appropriate security and privacy controls are planned and implemented accordingly.

49. Developing a system security plan or reviewing and approving any system security plan.

50. Assisting in determining the system boundary.

51. Preparing Privacy Threshold Assessments (PTAs), Privacy Impact Assessments (PIAs) as needed and SORNs.

52. Reviewing non-archived holdings of all personally identifiable information and ensuring, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reducing them to the minimum necessary for the proper performance of a documented agency function.

53. Reviewing the use of social security numbers in agency operational systems and programs to identify instances in which collection or use of the social security number is superfluous.

54. Establishing, and documenting in the security authorization package, interconnection agreements with other systems that specify security and privacy controls and responsibilities for the interconnected systems.

55. Deciding who should have access to the information and what their system privileges or access rights should be.

56. Assisting in the identification and assessment of the common security and privacy controls where the information resides.

57. Complying with the requirement for reviews of personally identifiable information retained by information system.

58. Maintaining all records which are used by the Agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

59. Establishing appropriate administrative, technical, and physical safeguards to ensure the security and privacy and confidentiality of records and to protect against any anticipated threats or hazards to their security, personal information or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.

60. Ensuring risk monitoring and data from the continuous monitoring tools are used to assess system risk on an ongoing basis.

61. Performing a criticality analysis to identify critical system components and functions when an architecture or design is being developed, modified, or upgraded.

62. Reflecting planned architecture changes in security and privacy plans.

63. Developing and maintaining a current inventory of the system components, information processing and storage location, and users that have access.

64. Developing, reviewing, and updating a supply chain risk management plan (SCRMP) for each system.

65. Ensuring the SCRMP is protected from unauthorized disclosure and modification.

66. Establishing a supply chain risk management team that includes IT and Business/Mission personnel to develop and maintain a SCRMP for the system. [SR-2(1)]

67. Establishing processes to identify and address weaknesses or deficiencies in the supply chain elements and processes in coordination with the Business/Mission owner.

68. Establishing controls to protect against supply chain risks to the system.

69. Documenting the selected and implemented supply chain processes and controls in the SCRMP.

70. Including Supply Chain Risk Management requirements in contracts for IT systems and services.

71. Assessing and reviewing the supply chain-related risks associated with suppliers or contractors for each system.

72. Establishing agreements and procedures, with entities involved in the supply chain, requiring systems to include, at least, notification of supply chain compromises and results of assessments or audits.

73. Developing criteria for inspection of the system or system components associated with Supply Chain Risk Management to detect tampering.

74. Developing and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system.

75. Reporting counterfeit system components to the source of counterfeit component and to the ACISO.

76. Training Forest Service personnel to detect counterfeit system components including hardware, software, and firmware.

77. Maintaining configuration control over the following identified system components awaiting service or repair and serviced or repaired components awaiting return to service.

78. Ensuring proper disposal of system data, documentation, tools, and system components in accordance with Forest Service policy.

6682.04f - Information System Security Officer

Each Information System Security Officer is responsible for the following in each system to which they are assigned:

1. Participating in system development by identifying appropriate security baseline configurations.

2. Periodically reviewing and validating system security and privacy controls to ensure they are in place and operating as intended.

3. Evaluating the impact on system security and privacy of proposed changes.

4. Providing technical advice for all security-related issues.

5. Monitoring the day-to-day security of systems, including physical and logical authorization and access, incident response, compliance with requirements for protecting the confidentiality of personally, identifiable information (PII), and awareness training and education.

6. Identifying, in conjunction with the information system change management process, pending system or environmental changes that may necessitate reauthorization of the system.

7. Reporting the status of Information System Security Officer (ISSO)-related tasks necessary to remediate identified system vulnerabilities are correctly and timely reported in the designated departmental or Forest Service Federal Information Security Management Act (FISMA) plan of action and milestones (POA&M) repository, as required.

8. Participating in and providing security-related input to the information system change management process.

9. Ensuring that any and all system changes are approved and done in accordance with FSM 6682.6b. Preventing, to the extent practical, unapproved system changes.

10. Assisting, with evaluation of proposed configuration changes to determine if the changes could harm system security and privacy properties as required.

11. Assisting, with development of an information system CM plan, as necessary.

12. Using data from the Agency dashboard to assess risk on an ongoing basis.

6682.04g - Information System or Application Program Managers and Application Developers

Information system or application program managers and application developers are responsible for:

1. Designing information systems to implement security and privacy controls based on the security categorization of the system and the confidentiality impact level of any personally identifiable information (PII) collected and/or retained by the system.

2. Designing into any application the security and privacy controls required by the current version of NIST SP 800-53 and those security controls necessary to minimize the need for separation of duties.

3. Developing and updating, as needed, a system security and privacy architecture, identifying critical system components and functions.

4. Conducting a RA and SCRA during initial information system design and immediately following any design changes during the life of an information system. Identifying the system's critical operational control functions, processes, and data.

5. Supporting the Forest Service risk management program by:

    a. Assisting with risk and supply chain risk assessment activities as needed.

    b. Incorporating new management or technical controls as necessary to mitigate identified risks.

    c. Integrating risk and supply chain risk assessments into the application development process and deployment life cycle.

6. Identifying cost, schedule, and performance issues during initial development and acquisition of systems or applications they are responsible for.

7. Working in conjunction with the system owner with:

    a. Operating, maintaining, and disposing of their systems in accordance with the security plans and other documented security and privacy control requirements.

    b. Coordinating and supporting security assessment and authorization for their systems, including reviewing the security authorization package before it is presented to the Certifying Official.

    c. Ensuring that the systems they manage provide required security and PII awareness training for system users and security support personnel.

8. Participating in PTA and PIA activities.

9. Preventing program execution in accordance with any agreements regarding software usage and restrictions and terms and conditions of software usage.

6682.04h - System Administrator

Administrators of information systems or applications are responsible for:

1. Making changes to the systems they administer only in accordance with FSM 6682.6b and preventing changes to hardware or software that have not been authorized in accordance with FSM 6682.6d.

2. Providing system configuration information as necessary in support of the Forest Service configuration and change management program.

3. Performing flaw remediation in accordance with FSM 6683.92.

4. Identifying and reporting to the ACISO and non-compliance with approved baseline configurations.

6682.04i - Procurement and Property Personnel and Grants Management Specialists

Forest Service Contracting Officers (CO), Purchasing Agents, Grants Management Specialists, and Real Property Leasing Officers are responsible for:

1. Requiring contractor or cooperator compliance with this directive when appropriate.

2. Ensuring that privacy, credentialing, and configuration management (CM) requirements are incorporated, as appropriate, into procurement requests/agreements and statements of work for information technology (IT) contracts and agreements.

3. Ensuring that solicitation documents/agreements (such as requests for proposals or requests for applications) for information systems and services include, either explicitly or by reference, applicable security and privacy requirements, including security and privacy controls as specified in the System Security Plan, or in applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4. Ensuring that requirements, in solicitation documents/agreements for information systems and services, permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented.

6682.04j - Investment Manager

The Investment Manager is responsible for:

1. Reviewing investments and providing business cases.

2. Ensuring that any products, procedures, or personnel (Federal employees and contractors) that are primarily dedicated to or used for the provision of IT security are explicitly identified as such in IT investment and capital budgeting documentation.

6682.04k - Contracting Officer, Contracting Officer Representative, and Sponsors

The Contracting Officer, Contracting Officer Representatives, and Forest Service Sponsors are responsible for:

1. Obtaining the system-specific rules of behavior on behalf of the contractor or cooperator.

2. Ensuring that contractors and cooperators sign the non-disclosure and any system-specific access agreements.

3. Returning original, signed non-disclosure and access agreement forms to the system owner when applicable.

4. Ensuring that the contract document includes all Federal Information System Security Act and associated NIST requirements.

6682.04l - Information System Users

Information System Users are responsible for:

1. Adhering to the Forest Service requirements regarding the use of Forest Service IT resources, data, and information systems specific rules of behavior for information systems to which they have been granted access.

2. Remaining fully aware of and abiding by Forest Service security policies as well as related Federal policy contained in the Privacy Act, Freedom of Information Act, and Forest Service IT policy.

3. Requesting a formal waiver that includes compensating controls for any requirement of FSM 6680 which they cannot comply.

4. Promptly reporting any incident where personally identifiable information or other sensitive agency data may have been lost, stolen, or compromised.

5. Not disclosing any personal information contained in any system of records except as authorized.

6. Protecting and properly disposing of any and all media, including portable and removable devices, that may contain sensitive information and promptly reporting any incident where media protection requirements may have been compromised to their Supervisor and to USDA CIRRB.

6682.05 - Definitions [Reserved]

6682.06 - References [Reserved]

6682.07 - Team, Committee, and Group Roles

6682.07a - Risk Assessment Team

The role of the Risk Assessment (RA) team is to:

1. Perform threat and vulnerability monitoring in conjunction with the USDA Cybersecurity Incident Response and Recovery Branch (CIRRB) and in accordance with U. S. Department of Agriculture (USDA) directives.

2. Conduct risk assessments (RAs) in accordance with NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments or Departmental Regulation (DR) 3540-003, Security Assessment and Authorization.

3. Utilize data classification and asset valuation in accordance with Federal Information Processing Standards (FIPS) 199 in performing RAs.

4. Ensure that gap analysis is included in all mitigation strategies and identify other risk management deficiencies.

5. Meet with Forest Service Business Managers and technical experts to identify and discuss mitigation needs identified in the system's Security Assessment Report, including any potential Forest Service-wide mitigation needs.

6. Develop processes with the Office of Inspector General (OIG) to share information regarding continuous monitoring results and their impact to security control assessments.

7. Identify reporting requirements for use in automated control assessment.

8. Determine how continuous monitoring results will be used in ongoing authorization (refer to NIST SP 800-137 Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, September 2011).

9. Produce a control assessment report and provide to system owner and authorizing official.

6682.1 - Risk Assessment and Update

1. Perform, review, or update Risk Assessment (RA) and Supply Chain Risk Assessment (FSM 6682.9).

    a. In accordance with USDA requirements or when there is a significant change to the system, information technology (IT) environment that could potentially affect the system's security and privacy status. [RA-3]

    b. On all new systems prior to implementation. [RA-3]

    c. On all new or modified images prior to installation on Forest Service workstations. [RA-3]

    d. In accordance with direction provided in NIST SP 800-30 Rev. 1, Guide for Conducting Risk Assessments and DR 3540-003, Security Assessment and Authorization. [RA-3]

2. Assess risks and implement security and privacy controls commensurate with the risks for:

    a. Access to Forest Service information systems by third parties.

    b. Duties and areas of responsibility that are incompatible.

3. Include an audit of security and risk mitigation controls in each RA.

4. Respond to findings from the RA, monitoring, and audits by determining an appropriate response to the risk. Acceptable responses are to accept the risk, transfer the risk, mitigate the risk, or generate a POA&M. [RA-7]

5. To accept the risk, perform a RA before approving a security policy waiver through an approved RBD.

6. Document the results in Cyber Security Assessment and Management (CSAM) repository, the department's official Federal Information Security Management Act (FISMA) reporting tool, in accordance with USDA requirements.

7. Disseminate risk and supply chain risk assessment results to appropriate personnel.

8. Perform a security categorization of the system using NIST SP 800-60 Rev. 1 in accordance with Federal Information Processing Standards (FIPS) Publication (Pub)

199 as required or whenever there is a change to information types processed by the system. [RA-2]

a. Any information processed, stored, or transmitted by the system is subject to this categorization.

b. Ensure the security categorization of any system processing, storing, or transmitting controlled unclassified information (CUI) is at least moderate confidentiality impact level.

b. Document the results of this categorization (including supporting rationale) in the system security plan and approved by designated senior-level Forest Service officials. [RA-2]

6682.2 - Security Controls Review [Reserved]

6682.3 - System Development Life Cycle Security Planning

1. Incorporate security requirements and controls into the system development life cycle (SDLC) of all Forest Service information systems in accordance with USDA Departmental Manual (DM) 3575-001. [SA-3]

    a. Select a control baseline for the system and tailor the selected controls by identifying and designating common controls, applying scoping considerations, selecting compensating controls, assigning values to control parameters, supplementing the control baseline with additional controls as needed, and providing information for control implementation. [PL-10, PL-11]

    b. Integrate security and privacy controls from inception for new systems or during the current life cycle phase for existing systems along with sufficient resources to adequately protect the information system. [SA-3]

    c. At a minimum, incorporate the security steps listed in exhibit 01 - Security Controls in the System Development Life Cycle.

    d. Define and document information system security and privacy roles and responsibilities throughout the system life cycle. [SA-3]

2. Coordinate the SDLC security planning with the CPIC process to avoid unnecessary duplication of steps or activities using NIST SP 800-37 Rev. 2. Phases to be coordinated are shown in exhibit 02, Information Security Relationships/Life Cycle Phases. [SA-3]

3. Develop security and privacy architectures for each system that: [PL-8]

a. Describe the requirements and approach to be taken for protecting the confidentiality, integrity, and availability of organizational information.

b. Describe the requirements and approach to be taken for processing personally identifiable information to minimize privacy risk to individuals.

c. Describe how the architectures are integrated into and support the enterprise architecture (EA); and

d. Describe any assumptions about, and dependencies on, external systems and services.

e. Use Zero Trust Architecture (ZTA) principles whenever possible.

4. Identify critical system components and functions by performing a criticality analysis for information systems, system components, or system service when an architecture or design is being developed, modified, or upgraded. [RA-9]

5. Review and update the architectures to reflect changes in the enterprise architecture. [PL-8]

6. Reflect planned architecture changes in security and privacy plans, Concept of Operations (CONOPS), criticality analysis, organizational procedures, and procurements and acquisitions. [PL-8]

7. Limit PII being processed throughout the information life cycle to the elements specified in the Privacy Impact Analysis (PIA). [SI-12(1) PRIV]

6682.3 - Exhibit 01

Summary of Security Controls in the System Development Life Cycle

Phase	Control	Details
INITIATION	Initiate Security Planning	Identification of security roles, stakeholder security integration awareness, and initial project planning.
INITIATION	Categorize the Information System	Determine category in accordance with Federal Information Processing Standard (FIPS) 199.
INITIATION	Assess Business Impact	Assessment of security impact on lines of business in correlation with system-specific components with critical business services.
INITIATION	Assess Privacy Impact	Consideration of what information the system will transmit, store, or create that may be considered privacy information.
INITIATION	Ensure Use of Secure Information System Development Processes	Secure Concept of Operations (CONOPS) for Development, Standards and Processes, Security Training for Development Team, Quality Management, Secure Environment, Secure Code Practices and Repositories.
DEVELOPMENT/ ACQUISITION	Assess Risk to System	Evaluate current knowledge of the system's design, stated requirements, and minimum-security requirements derived from the security categorization process to determine their effectiveness to mitigate anticipated risks.

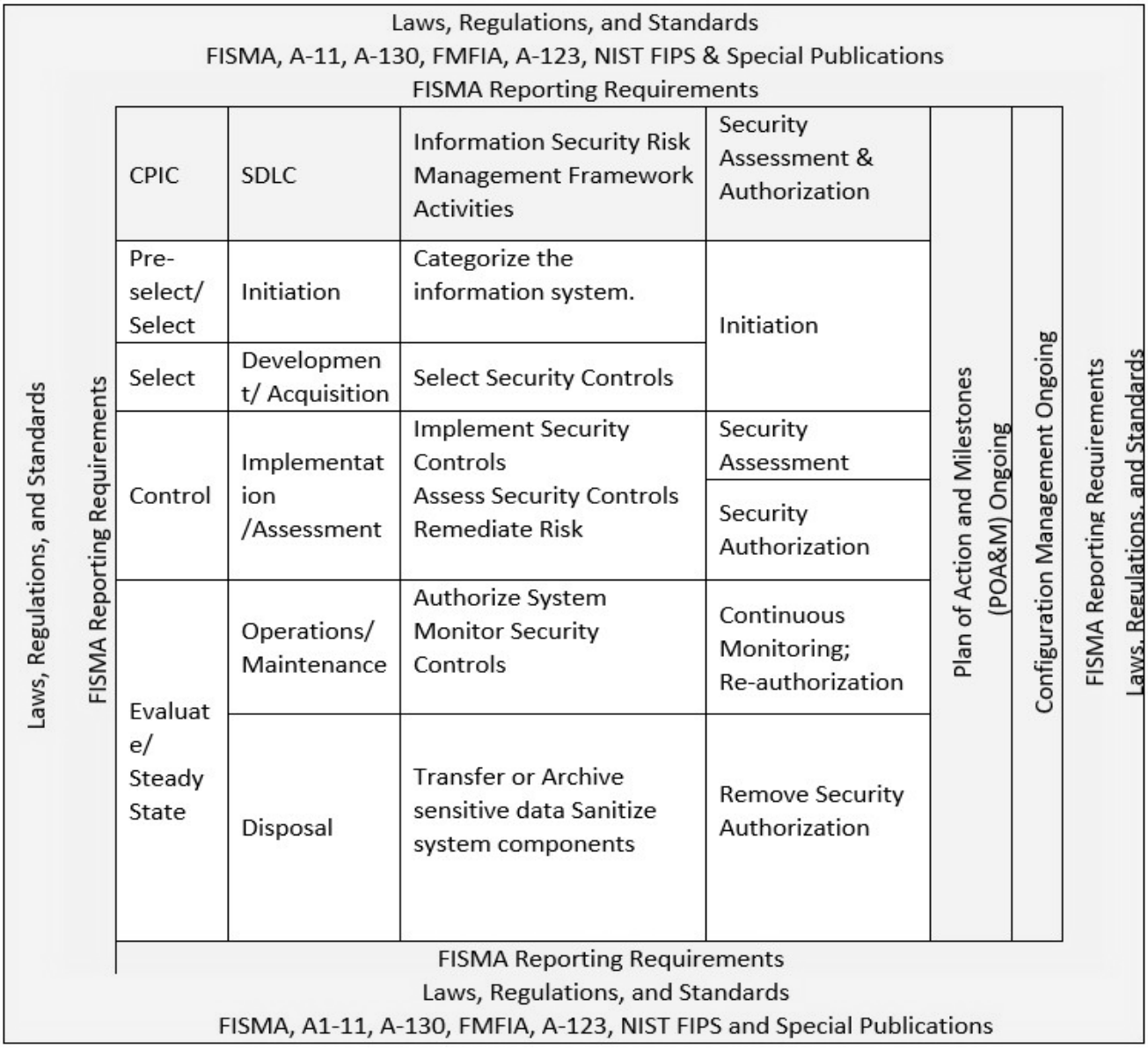
Phase	Control	Details
IMPLEMENTATION/ ASSESSMENT	Select and Document Security Controls	1. Selection of baseline security controls (including common controls). 2. Application of security tailoring guidance to adjust to initial security control baseline. 3. Supplementation of the tailored baseline with additional controls based on an assessment of risk and local conditions.
IMPLEMENTATION/ ASSESSMENT	Design Security Architecture	Identification of shared service providers and centralization of key security services within agencies.
IMPLEMENTATION/ ASSESSMENT	Engineer in Security and Develop Controls	Security controls are implemented and become part of the information system rather than applied at completion.
IMPLEMENTATION/ ASSESSMENT	Develop Security Documentation	Configuration Management Plan; Contingency Plan (including Business Impact Assessment); Continuous Monitoring Plan; Security Awareness, Training, and Education Plan; Incident Response Plan; and Privacy Impact Assessment.
IMPLEMENTATION/ ASSESSMENT	Conduct Testing (Development, Functional, and Security)	Information systems developed or undergoing software, hardware, and/or communication modification(s) must be tested and evaluated prior to being implemented.

Phase	Control	Details
IMPLEMENTATION/ ASSESSMENT	Create a Detailed Plan for SAA	Develop an Initial Work Plan in identifying key players, project constraints, core components, scope of testing, and level of expected rigor.
IMPLEMENTATION/ ASSESSMENT	Assess System Security	Validate that the information system complies with the functional and security requirements and will operate within an acceptable level of residual security risk.
IMPLEMENTATION/ ASSESSMENT	Authorize the Information System	The authorization, granted by a senior agency official, is based on the verified effectiveness of security controls to some agreed-upon level of assurance and an identified residual risk to agency assets or operations (including mission, function, image, or reputation). Ensure that security controls are in place, effective, and operating as intended.
OPERATION/ MAINTENANCE	Review Operational Readiness	Evaluate the security implications due to any system changes.
OPERATION/ MAINTENANCE	Perform Configuration Management and Control	Change Control Board decisions, updated SSPs and POA&Ms, security evaluations of documented system changes.
OPERATION/ MAINTENANCE	Conduct Continuous Monitoring	Provides system owners with effective tools and dashboards for producing ongoing updates to SSPs, SARs, and POA&Ms and to maintain near real-time security status.

Phase	Control	Details
DISPOSAL	Build and Execute a Disposal/Transition Plan	Ensures all stakeholders are aware of the future plan for the information system and its information. Verify all records management and retention requirements. Note: Do not dispose of any record that is subject to litigation hold or record retention requirements.
DISPOSAL	Ensure Information Preservation	Consideration of the methods that will be required for retrieving information in the future.
DISPOSAL	Sanitize Media	Development of media sanitization records.
DISPOSAL	Dispose of Hardware and Software	Development of disposition records for hardware and software.
DISPOSAL	Closure of System	Documentation verifying system closure, including final closure notification to the authorizing officials, configuration management, information system owner, ISSO, and Program Manager.

6682.3 - Exhibit 02

Information Security Relationships/Life Cycle Phases



6682.4 - Security Assessment and Authorization Policies

1. Review and update the current assessment and authorization (A&A) policy and procedures as required. [CA-1]

2. Conduct security A&As in accordance with the current USDA Risk Management Framework (RMF) guidelines and other current Federal, Departmental, and Forest Service regulations. The security assessment and authorization of a GSS covers the applications and information systems that execute on the GSS only if: [CA-2]

    a. The security controls applicable to the application or information system are identical to or are a subset of the GSS security controls.

    b. All software and hardware used by the application or information system is also included in the SAA of the GSS.

3. Designate an information system security officer (ISSO) for each GSS, major application (MA), and, if applicable, their respective component subsystems and applications. [CA-1]

4. Ensure that all identified security program and system security deficiencies and mitigating actions are tracked electronically with an approved tracking system.

5. Ensure that information systems, including cloud systems developed or operated by third parties on behalf of the Forest Service have undergone processes equivalent to the Forest Service continuous A&A process or otherwise substantially comply with the requirements of this chapter.

6. Ensure that an information system that will be used to conduct or host information collection from the public is properly authorized to operate, and has obtained appropriate OMB clearance, prior to such collection.

6682.4a - Security Control Assessments

1. Complete a security assessment for all general support systems (GSSs), major applications and contractor provided systems, including cloud systems in accordance with USDA requirements or when a significant change occurs to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome for meeting the security requirements for the system. [CA-2]

2. Develop a security assessment plan that describes the scope of the assessment, the assessment environment, assessment team, and assessment roles and responsibilities in accordance with USDA requirements and is approved by the authorizing official or their representative. [CA-2]

3. Produce a control assessment report and give to the system owner and authorizing official. [CA-2]

4. Employ an independent assessor or assessment team to conduct assessment of the security controls in each FIPS 199 moderate or high impact information system. Independent assessors must be free from any perceived or actual conflicts of interest with regard to the development, operation, or management of the Forest Service information system under assessment in order to determine security control effectiveness. [CA-2(1)]

5. Perform a security assessment on financially significant systems. [CA-2]

6682.4b - Information Exchange

1. Allow connections from Forest Service information systems to other information systems only when authorized and documented in an Agreement and associated Memorandum of Understanding (MOU). The types of agreements selected are based on factors such as the impact level of the information being exchanged, the relationship between the organizations exchanging information (such as, government to government, government to business, business to business, government or business to service provider, government or business to individual), or the level of access to the organizational system by users of the other system. [CA-3]

2. If systems that exchange information have the same authorizing official, the systems need not develop agreements. Instead, the interface characteristics between the systems (such as, how the information is being exchanged. how the information is protected) are described in their respective security and privacy plans. [CA-3]

3. Employ a deny-all, permit-by-exception policy for allowing Forest Service information systems to connect to external information systems and execution of authorized software on Forest Service information systems. [CM-7(5)]

4. Establish a process for requesting connections to non-Forest Service information systems through the configuration management (CM) and change control process.

5. Develop an Agreement in accordance with USDA Guidelines that sets out the terms of the interconnection, the interface characteristics, security requirements, the nature of the information communicated, agreed to configurations and security controls, and dates when the connections and the security controls must be in place. [CA-3, CA-9]

6. If PII is permitted to be transferred or accessed via the interconnection, include requirements for safeguarding the PII. [CA-3]

7. Maintain an active, current list of all interconnections.

8. Review and update system interconnections in accordance with the Agreement and verify enforcement of security requirements. Terminate the Agreement when connection is no longer needed. [CA-3, CA-9]

9. Interconnected systems shall contain nondisclosure language in the Agreement and require a nondisclosure agreement to be signed by contractors who will access Forest Service information systems or information.

6682.4c - Plan of Action and Milestones

1. Develop and update a plan of action and milestones (POA&M) process for the information system that documents the Agencies' planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security and privacy controls and to reduce or eliminate known vulnerabilities in the system. All deficiencies must be recorded in the Forest Service automated tool. [PM-4]

2. Ensure that all POA&Ms follow the process, specifications, and reporting schedule of USDA. [CA-5]

3. Ensure that all POA&Ms include all IT security program-level and system-level weaknesses identified from but not limited to the following sources: [CA-5, PM-4]

    a. Office of Inspector General (OIG) reports,

    b. General Accounting Office (GAO) reports

    c. All security control assessment reports (such as, Department Compliance Review reports, or reports of contractors hired by the operating unit to conduct IT security self-assessments or vulnerability scans) and continuous monitoring activities; and

    d. Security Impact Assessments (SIA).

4. Implement corrective actions to address weaknesses. [CA-5]

5. Review corrective action status and update in accordance with USDA requirements. [CA-5, PM-4]

6682.4d - Security Authorization

1. Authorize the information system for processing by issuing an authorization to operate (ATO) before operations and update the authorization in accordance with

USDA requirements, when there is a significant change to the system, or when directed by the AO. [CA-6]

2. For each system or application that is authorized, assign: [CA-6]

    a. An AO who is a program area Line Officer with the authority to evaluate the mission, business case and budgetary needs for the system in view of the security risks. [CA-6]

    b. An independent assessor who is impartial and not influenced by the system owner, application developers or AO. [CA-2(1), CA-7(1)]

6682.4e - Continuous Monitoring

1. Follow the USDA continuous monitoring strategy outlined in the current USDA Risk Management Framework (RMF) guidelines and monitor the Forest Service information security program and all information systems for effectiveness and adequacy of system controls in accordance with appropriate NIST guidance. [CA-7]

2. Ensure risk monitoring is part of the information security continuous monitoring strategy. [CA-7(4)]

3. Perform ongoing security control assessments in accordance with USDA's designated continuous monitoring strategy (FSM 6682.4) and utilize automated processes when available. [CA-7]

4. Perform ongoing security status monitoring of Forest Service-defined metrics in accordance with the information security continuous monitoring strategy (FSM 6682.4e). [CA-7]

5. Report the security state of the information system to the AO and other appropriate officials through the use of the agency dashboard and in accordance with the information security continuous monitoring strategy (FSM 6682.4e) or as directed by the ACISO. [CA-7]

6. Follow USDA, or develop and maintain a Forest Service level, ISCM strategy as per the OMB Memorandum M-14-03. Implement the ISCM strategy in accordance with USDA Guidance.

6682.5 - Security Planning

6682.5a - System Security and Privacy Plans and Rules of Behavior

1. Develop a System Security and Privacy Plan (SSP) in accordance with departmental guidance (USDA DR 3540-003 and current USDA Risk Management Framework (RMF) guidelines) for each: [PL-2]

    a. General support system (GSS) and its components (OMB Circular A-130 (FSM 6680.01d)).

    b. Major application and its components (National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 Rev. 1, FSM 6680.06a). Other non-major applications should be covered by the system security and privacy plans and security controls for the GSS in which they operate.

    c. Non-Federal system that supports a federal function (NIST SP 800-18 Rev.1, FSM 6680.06a).

2. Ensure that SSPs are reviewed in accordance with USDA requirements and updated if a significant change to the system or IT environment occurs which affects the system's security posture. (NIST SP 800-18 Rev.1, referenced in FSM 6680.06a.) [PL-2]

3. Ensure that SSPs are protected from unauthorized disclosure and modification. [PL-2]

4. Ensure that system-related documentation is available, protected as required, and distributed to authorized personnel. [PL-2]

5. Plan and coordinate security-related activities affecting the information system.

6. Establish system rules of behavior in accordance with FSM 6682.5a and the guidelines set forth in NIST SP 800-18 Rev. 1 and make these rules readily available to all individuals requiring access to Forest Service information systems. Include, in the rules of behavior, restrictions on use of social media, social networking sites, and external sites/applications, posting organizational information on public websites, and use of email addresses and passwords for creating accounts on external sites/applications.
   [PL-4, 4(1)]

7. Execute required security agreements incorporating system rules of behavior in accordance with FSM 6683.23e, Security Responsibility Access Agreements. [PL-4]

8. Review and update the system rules of behavior in accordance with FSM 6683.23e, Security Responsibility Access Agreements. [PL-4]

9. Require individuals who have signed a previous version of the system rules of behavior to read and re-sign a current version of them whenever the rules of behavior are revised/updated. [PL-4]

6682.6 - Configuration Management

1. Ensure all employees, contractors, partners, and volunteers responsible for development or maintenance of Forest Service systems follow Forest Service configuration management practices in accordance NIST SP 800-128.

2. Ensure employees, partners, and volunteers are prohibited from downloading software or connecting hardware unless pre-approval has been granted and documented.

3. Monitor CM policy compliance using continuous monitoring within the organization-defined frequency.

4. Establish the scope of authority of the change management process through an approved charter.

5. Ensure security and privacy representatives are members of the Forest Service Change Control Board. [CM-3(4)]

6682.6a - Baseline Configuration

1. Develop, document, and maintain, under configuration control, a current system baseline configuration after the completion of a formal review at the end of each life cycle phase. [CM-2]

2. Develop, review, and update the list of authorized software programs. [CM-7(5])

3. Maintain the currency, completeness and accuracy of the baseline configuration using automated tools. [CM-2(2)]

4. Review and update the baseline to reflect approved changes to the system or specific configuration item in accordance with USDA requirements. [CM-2]

5. Retain previous versions of the baseline configurations to support rollback. [CM-2(3)]

6. Issue necessary system components or devices to individuals traveling to locations that the Forest Service deems to be of significant risk. [CM-2(7)]

7. Apply appropriate security safeguards to the system components or devices when the individuals returning from traveling to locations that the Forest Service deems to be of significant risk. [CM-2(7)]

6682.6b - Configuration Change Control

1. Determine the types of changes to the information system that are configuration controlled. [CM-3]

2. Review and approve configuration-controlled changes to the system with explicit consideration for the Security and Privacy Impact Analyses. [CM-3]

3. Document all approved configuration-controlled changes to the system. [CM-3]

4. Retain and review records of configuration-controlled changes to the system, in accordance with USDA policy and Forest Service records retention requirements. [CM-3]

5. Audit and review activities associated with configuration-controlled changes to the system. [CM-3]

6. Coordinate and provide oversight for configuration changes control through a chartered configuration control entity, the Change Control Board (CCB). The frequency and conditions that prompt the change control element to convene are to be identified within the charter in accordance with USDA requirements for the USDA Enterprise Configuration and Change Management Change Advisory Board (CAB). [CM-3]

7. Test, validate, and document configuration setting changes to the information system before implementing the changes on the operational system. [CM-3(2)]

6682.6c - Impact Analyses

1. Assess and document in an impact analysis the potential security and privacy impacts of proposed configuration changes prior to implementation. [CM-4]

2. Review and approve any changes to be made to Forest Service information systems. [CM-4]

3. Monitor implemented changes for unexpected security and privacy impacts and for opportunities to improve the effectiveness of security controls. [CM-4(2)]

4. Retain documentation of all impact analyses.

6682.6d - Access Restrictions for Change

1. Harden operating systems to the maximum extent and configure to prevent circumvention of information technology (IT) security controls.

2. Prevent unauthorized access to application configurations.

3. Store and control the contents of software code and system technical documentation in a system software repository.

4. Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. [CM-5]

6682.6e - Configuration Settings

1. Establish and document mandatory configuration settings with the baseline from the NIST SP 800-70 Rev. 4 National Checklist Program for IT Products in accordance with USDA requirements for information technology (IT) products employed within the information system. [CM-6]

2. Configure the security settings of IT products to the most restrictive mode consistent with operational requirements. [CM-6]

3. Document and approve the configuration settings and all deviations from the established configuration settings for individual components within the information system based on explicit operational requirements. [CM-6]

4. Deploy and utilize approved Forest Service tools for configuration settings management for enforcement of configuration settings, baseline and identification of vulnerabilities where appropriate. [CM-6(1)]

5. Monitor and control changes to the configuration settings in accordance with organizational requirements. [CM-6]

6. Incorporate detection of unauthorized, security-relevant configuration changes into the system's operational procedures and processes and incorporate them into the system's incident detection process.

6682.6f - Least Functionality

1. Configure information systems to provide only essential capabilities. [CM-7]

2. Prohibit or disable, as appropriate, the use of specific functions, ports, protocols, and/or services not supporting those essential capabilities. [CM-7]

3. Document in the System Security Plan (SSP), in accordance with USDA requirements, a listing of essential ports, protocols, and services.

4. Review, in accordance with USDA requirements, the listing of essential ports, protocols, and services. [CM-7(1)]

5. Limit component functionality to a single function per device, where feasible.

6. Document and retain all hardening guidelines and best practices employed.

7. Develop and maintain the baseline configuration. [CM-2]

8. Prevent program execution in accordance with agreements regarding software usage and restrictions and in terms and conditions of software usage. [CM-7(2), CM-10]

6682.6g - System Component Inventory and Information Location

1. Utilize continuous monitoring capabilities for hardware asset and software asset management and information location. [CM-12(1)]

2. Develop and maintain a current inventory of the system components, information processing and storage location, and users that have access to the information for each Forest Service system. [CM-8, CM-12]

3. Ensure component inventories are consistent with the authorization boundary of the information system. [CM-8]

4. Update the inventory of system components and location of information as a part of component installation, removal, and system updates. [CM-8(1), CM-12]

5. Review the information system component inventory and information location for accuracy in accordance with the organization defined frequency. [CM-8, CM-12]

6. Ensure that the information system component inventory is available for review and audit by designated Forest Service officials.

7. Employ mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the system.

8. When an unauthorized component is detected, take action to disable network access by such components and/or isolate the components and invoke the incident response procedures. [CM-8(3)]

6682.6h - Configuration Management Plan

1. Ensure that a configuration management plan (CMP) is developed, documented, protected from unauthorized disclosure and modification, and implemented that: [CM-9]

    a. Addresses roles, responsibilities, and configuration management processes and procedures.

    b. Defines the configuration items, system components and information location for the system and when in the SDLC the configuration items are placed under configuration management. [CM-12]

    c. Establishes the means for identifying configuration items throughout the SDLC and a process for managing the configuration of the configuration items.

2. Ensure that each CMP is protected from unauthorized disclosure and modification. [CM-9]

6682.7 - System Documentation

1. Obtain and protect all system administration documentation for a Forest Service information system, system component, or system service and make available to system administrators in accordance with risk management strategies. [SA-5]

2. Obtain and protect all user documentation for a Forest Service information system, system component, or system service and make available to authorized personnel in accordance with risk management strategies. [SA-5]

3. Track changes to the information system, system component, or system service documentation and attempts to obtain system documentation when the documentation is unavailable or nonexistent. [SA-5]

4. Provide adequate documentation to appropriate system personnel, in incident response situations, and at alternate information system operating sites in accordance with the system's contingency plan. [SA-5]

6682.8 - Supply Chain Risk Management

1. Develop, review, and update a supply chain risk management plan (SCRMP) for each system. [SR-2a, b]

2. Ensure the SCRMP is protected from unauthorized disclosure and modification. [SR-2c]

3. Establish a supply chain risk management team that includes IT and Business/Mission personnel to develop and maintain a SCRMP for the system. [SR-2(1)]

4. Establish processes to identify and address weaknesses or deficiencies in the supply chain elements and processes in coordination with the Business/Mission owner. [SR-3a]

5. Establish controls to protect against supply chain risks to the system. [SR-3b]

6. Document the selected and implemented supply chain processes and controls in the SCRMP. [SR-3c]

7. Include Supply Chain Risk Management requirements in contracts for IT systems and services. [SR-5]

8. Assess and review the supply chain-related risks associated with suppliers or contractors for each system. [SR-6]

9. Establish agreements and procedures, with entities involved in the supply chain, requiring systems to include, at least, notification of supply chain compromises and results of assessments or audits. [SR-8]

10. Develop criteria for inspection of the system or system components associated with Supply Chain Risk Management to detect tampering. [SR-10]

11. Develop and implement anti-counterfeit policy and procedures that include the means to detect and prevent counterfeit components from entering the system. [SR-11a]

12. Report counterfeit system components to the source of counterfeit component and to the ACISO. [SR-11b]

13. Train Forest Service personnel to detect counterfeit system components including hardware, software, and firmware. [SR-11(1)]

14. Maintain configuration control over the following identified system components awaiting service or repair and serviced or repaired components awaiting return to service. [SR-11(2)]

15. Ensure proper disposal of system data, documentation, tools, and system components in accordance with Forest Service policy. [SR-12]

6682.9 - Additional Security Management Controls for High Value Asset Systems

Note: These policies only apply to information systems designated by USDA as a High Value Asset (HVA) System.

6682.9a - Joint Authorization

Employ a joint authorization process for the system that includes multiple authorizing officials from the same organization conducting the authorization. [CA-6(1)]

6682.9b - Continuous Monitoring Trend Analyses

Employ trend analyses to determine if control implementations, the frequency of continuous monitoring activities, and the types of activities used in the continuous monitoring process need to be modified based on empirical data. [CA-7(3)]

6682.9c - Defense-In-Depth in Security and Privacy Architectures

Design the security and privacy architectures for the system using a defense-in-depth approach that: [PL-8(1)]

1. Allocates multiple controls to different locations and architectural layers; and

2. Ensures that the allocated controls operate in a coordinated and mutually reinforcing manner.

6682.9d - Vulnerability Monitoring and Scanning

1. Compare the results of multiple vulnerability scans using Forest Service-approved automated trend analysis tools to determine trends in system vulnerabilities and identify patterns of attack. [RA-5(6)]

2. Correlate the output from vulnerability scanning tools to determine the presence of multi-vulnerability and multi-hop attack vectors. [RA-5(10)]

6682.9e - Developer Testing and Evaluation

1. Require the developer of the system, system component, or system service to employ static code analysis tools to identify common flaws and document the results of the analysis. [SA-11(1)]

2. Require the developer of the system, system component, or system service to perform threat modeling and vulnerability analyses during development and the subsequent testing and evaluation of the system, component, or service that: [SA-11(2)]

a. Uses contextual information provided by the System Owner.

b. Employs tools and methods approved by the Assistant Chief Information Security Officer (ACISO) for Natural Resources and Environment (NRE); and

c. Conducts the modeling and analyses at a level of rigor approved by the ACISO for NRE; and

d. Produces evidence that meets acceptance criteria approved by the ACISO for NRE.

3. Require the developer of the system, system component, or system service to perform a manual code review of critical software and firmware components of systems designated by the System Owner using processes, procedures, and/or techniques approved by the ACISO for NRE. [SA-11(4)]

4. Require the developer of the system, system component, or system service to perform penetration testing at a level of rigor and under constraints determined by the ACISO for NRE. [SA-11(5)]

5. Require the developer of the system, system component, or system service to employ dynamic code analysis tools to identify common flaws and document the results of the analysis. [SA-11(8)]

6682.9f - Supply Chain Provenance

1. Establish and maintain unique identification of systems and critical system components for tracking through the supply chain. [SR-4(2)]

2. Employ controls to validate that the system or system component received is genuine and has not been altered. [SR-4(3)].

6682.9g - Assessments Prior to Selection, Acceptance, Modification, or Update

Assess the system, system component, or system service prior to selection, acceptance, modification, or update to uncover evidence of tampering, unintentional and intentional vulnerabilities, or evidence of non-compliance with supply chain controls. [SR-5(2)]

6682.9h - Tamper Resistance and Detection

Implement a tamper protection program for the system, system component, or system service. [SR-9]

6683 - Security Operational Controls

6683.01 - Authority [Reserved]

6683.02 - Objective

The objective of operational security controls is to protect the confidentiality, integrity, and availability of the information, information systems, and information technology (IT) that support the Forest Service mission by:

1. Mitigating risks to Forest Service information, physical resources, operation, or image that can result either intentionally or accidentally from insufficiently secured or inappropriately used IT resources.

2. Ensuring that employees are clearly and explicitly informed about requirements and procedures regarding the security and use of IT resources.

3. Providing an effective Forest Service response to security threats and breaches.

6683.03 - Policy [Reserved]

6683.04 - Responsibility

6683.04a - Assistant Chief Information Officer for Natural Resources and Environment

The Assistant Chief Information Officer (ACIO) for Natural Resources and Environment (NRE) has overall responsibility for the Forest Service's program and management of operational security controls for information, information systems, and IT.

The ACIO for NRE is responsible for:

1. Establishing an overall Forest Service IT security and privacy awareness and training strategy.

2. Ensuring that Forest Service IT security and privacy awareness and training programs are developed, implemented, documented, and maintained.

3. Working with the Forest Service Director of Human Resources Management (HRM) to ensure that problems or issues affecting information system personnel screening are promptly addressed and efficiently resolved.
4. Communicating with the United States Department of Agriculture, Office of the Chief Information Office (USDA, OCIO), as required by USDA DR 3505-005, regarding information system security incidents, responses, and follow-up actions.
5. Ensuring that the security and integrity of Forest Service information systems is protected by proper implementation of backup and recovery plans and procedures.

6683.04b - Assistant Chief Information Security Officer for NRE

The Assistant Chief Information Security Officer (ACISO) for NRE is responsible for:

1. Ensuring protection of evidence, forwarding, and coordinating immediately with the USDA, Chief Information Security Officer (CISO) or designated agent any suspected high-level, major IT security incidents that may be a violation of criminal law, including but not limited to the following:
    a. Distribution of copyrighted software,
    b. Child pornography,
    c. Sexually explicit material,
    d. Downloading of music or unauthorized software,
    e. On-line gambling, and
    f. Any violation of law.
2. Forwarding to the USDA, Office of the CISO all suspected incidents of copyright infringement or any other illegal activity involving information system resources.
3. Promoting awareness and understanding of the policies and issues related to appropriate use and limited personal use of telecommunications and IT resources and equipment.
4. Verifying that recovery procedures are tested as required and function as intended.
5. Recommending steps to address promptly and resolve problems or issues affecting information system personnel screening.
6. Coordinating with Human Resources Management, Procurement and Property Services and the Office of Grants and Agreements staffs to integrate information system user hiring, transfer, and termination procedures into applicable personnel and contract actions.

6683.04c - Information System Security Manager

Information System Security Managers are responsible for:

1. Ensuring protection of evidence, forwarding, and coordinating immediately with the Assistant Chief Information Security Officer (ACISO) for NRE any suspected high-

level, major IT security incidents that may be a violation of criminal law, including but not limited to the following:

a. Distribution of copyrighted software,

b. Child pornography,

c. Sexually explicit material,

d. Downloading of music or unauthorized software,

e. On-line gambling, and

f. Any violation of law.

2. Forwarding to the ACISO for NRE all suspected incidents of copyright infringement or any other illegal activity involving information system resources.

3. Verifying that Information System Contingency Plans (ISCPs) are developed for information systems and:

   a. Tested, reviewed, and updated as necessary for all other systems.

   b. Personnel with recovery responsibilities receive training regarding these responsibilities.

4. Verifying that information system contingency plans (ISCPs) for Forest Service information systems are developed and:

   a. Coordinated with other applicable emergency plans.

   b. Tested, reviewed, and updated as necessary as required.

   c. Quickly and efficiently executed.

5. Ensuring system owners and Managers understand the security training strategy.

6. Overseeing the development and implementation of the Forest Service IT security awareness and training programs.

7. Verifying that recovery procedures are tested as required and function as intended.

8. Assisting in identifying deficiencies in backup and recovery plans or procedures.

9. Recommending steps to address promptly and resolve problems or issues affecting information system personnel screening.

10. Assisting those involved in determining position sensitivity levels that are applicable to positions that develop, manage, support, maintain, operate, and use each Forest Service information system, and in the event of a dispute, making the final determination regarding the position sensitivity level to be applied to such a position.
11. Educating users about their responsibilities for maintaining effective media protection to prevent unauthorized user access.

6683.04d - Authorizing Official

The Authorizing Official is responsible for:

1. Ensuring personnel in their units receive required information security and privacy training.

2. Supporting or cooperating with the execution of ISCPs in the event of an emergency, disaster, or other major disruption of an information system.

3. Making an appropriate reassignment or terminating any employee who fails to receive a favorable adjudication as a result of the personnel screening process.

4. Making the final determination whether or not a given change continues to be an acceptable security risk.

6683.04e - System Owners

System owners are responsible for:

1. Supporting and participating, as required, in the role-based training of all personnel with regard to their additional information security and privacy roles and responsibilities.

2. Procuring, developing, integrating, modifying, operating, and maintaining the system owner's information systems.

3. Making corporate information available for backup.

4. Ensuring development of backup and recovery plans for their system(s).

5. Verifying that backup and recovery plans and procedures are followed, and backups are tested.

6. Reporting failures to follow backup and recovery plans and procedures to the Authorizing Official.

7. Resolving deficiencies in backup and recovery plans and procedures.

8. Participating, as required, in the development, review, approval, and testing of ISCPs for their systems.

9. Reviewing, approving, and participating in the testing of information system ISCPs that involve or affect resources or facilities for which they are responsible.

10. Assisting with the execution of ISCPs for their systems and the resulting response and recovery efforts.

11. Arranging for and funding any training necessary for all those with a role or responsibility in executing ISCPs for their system(s), to ensure the individuals understand both the plan(s) and their role(s).

12. Verifying and documenting the personnel screening of all those with access to their system.

13. Working with the Forest Service CIO Cybersecurity Internal Controls Branch Chief and Human Resources Management (HRM) officials to determine the position sensitivity levels that are applicable to positions that develop, manage, support, maintain, operate, and use their Forest Service information system.

14. Denying system access until appropriate personnel screening has been completed, unless the screening has been waived.

15. Implementing and documenting security or other compensating controls when separation of duties is not possible.

16. Requiring Supervisors to review new and changed position descriptions as part of the position classification process to ensure that the proper separation of duties is maintained and incorporate security and privacy roles and responsibilities into positions descriptions where needed.

17. Making, in cooperation with the Forest Service Director of HRM, the suitability determination for employees whose position or duties requires a higher level of personnel screening than has been previously conducted, but only for positions for which the Forest Service makes the final determination of suitability.

18. Maintaining a list of all authorized personnel who perform maintenance on information systems.

19. Ensuring that all removable media is labeled properly.

20. Using cryptographic methods to protect and restrict access to information on portable digital media and devices, preventing unauthorized disclosure and modification of information at rest.

21. Ensuring media is properly stored and transported.

22. Ensuring that litigation hold is considered before media is sanitized.

23. Verifying that media are sanitized before reuse or disposal.

24. Ensuring that least privilege is enforced on the information system.

25. Ensuring that all applicable maintenance security controls are implemented.

26. Ensuring that all maintenance tools (diagnostic and test tools, software, or equipment) and their use is monitored. In addition, ensuring that approved maintenance tool use is defined and documented in the System Security Plan (SSP).

27. Reporting to Law Enforcement and Investigations (LEI) incidents that may be a violation of criminal law, involve the theft or loss of IT hardware containing information, and/or incidents that may pose a threat to the safety of employees.

28. Overseeing the execution of ISCPs and any subsequent damage assessment and recovery efforts.

29. Managing and participating in the CCBs for systems and provide technical staff to conduct and/or review security impact analyses.

30. Incorporating flaw remediation into the system configuration management process and coordinating configuration management issues.

31. Ensuring that the security and integrity of Forest Service information systems is protected by proper implementation of backup and recovery plans and procedures.

32. Ensuring that appropriate training and certification opportunities are available to those with a role or responsibility in developing or implementing information system contingency plans.

33. Ensuring that IT contingency plans are developed and approved for all corporate information systems.

34. Ensuring that resources and facilities needed for disaster recovery and business resumption, such as alternate backup or operations sites, are available.

35. Approving the orderly disconnect or shutdown of compromised systems, if necessary, as a mitigating action, and the reactivation of those compromised systems after recovery.

36. Ensuring that mitigation of all incidents is completed, and preventive measures are taken to reduce incident recurrence.

37. Ensuring that any Forest Service IT system effectively implements and maintains IT security policies and procedures to address all media protection requirements.

38. Designating appropriate IT component teams to implement the system recovery strategy and ensure that each team should be trained and ready to deploy in the event of a disruptive situation requiring plan activation.

39. Establishing and implementing an internal Forest Service program for patch management on all information systems.

40. Clearly assigning System Administrators and other authorized personnel specific patch management and vulnerability correction responsibilities.

41. Employing the departmental or an approved automated patch management solution to facilitate compliance with this policy and to promote efficiency for all systems, wherever feasible; apply patch management solutions to in-house applications and monitor status of those systems.

42. Ensuring that the separation of duties is maintained for all critical operational and information security functions.

43. Verifying that all systems, applications, or point solution security plans include applicable backup and recovery strategies.

44. Ensuring formal procedures are in place to control the allocation of access rights to prevent unauthorized access or disclosure of media devices containing confidential or proprietary information.

45. Ensuring the monitoring of all media and media devices to detect deviation from established policies and record security events to provide evidence in the case of unauthorized access and/or security incidents.

46. Ensuring that only Forest Service approved hardware and software is used within the system boundaries.

47. Working with Information Technology Asset Managers to establish system-level reporting categories.

48. Working with the Procurement and Property Services and Grants and Agreements staff to include the security and privacy requirements, criteria, and/or specifications, as appropriate, explicitly or by reference, in the acquisition contract/agreement for the information system, system component, or information system service.

49. Implementing the privacy "principle of minimization" when processing PII.

50. Monitoring the system and all inbound and outbound communications traffic to detect attacks, indicators of potential attacks, unauthorized activities/conditions and local, network or remote connections and responding to any threats.

6683.04f - Information System Security Officers

Information System Security Officers (ISSO) are responsible for:

1. Subscribing to specific security and advisory alerts applicable to their IT system(s) that may not be included in information about common threats, vulnerabilities, and incident-related information disseminated by the CIO Cybersecurity Internal Controls branch.

2. Providing the CIO Cybersecurity Internal Controls branch with responses regarding actions taken in response to the security alerts or advisory alerts.

3. Assisting system owners in resolving deficiencies in backup and recovery plans or procedures.

4. Developing, updating, and maintaining the ISCPs as required.

5. Developing and conducting ISCP tests and completing associated test documentation as required.

6. Developing and updating ISCP training plans for their assigned information systems.

7. Supporting or participating in the training of contingency personnel as required by a specific plan.

8. Supporting the Forest Service IT security awareness and training strategy and fostering an atmosphere of IT security in general.

9. Notifying the system owner of any conflicts or discrepancies between Forest Service-wide directives or procedures, and individual system security plan requirements, and helping to resolve such conflicts.

10. Providing Information System, Network, and Security Administrators of the Forest Service information systems or networks for which the ISSO is responsible, direction to grant, modify, disable, or terminate user access rights.

11. Assisting or coordinating assistance to the USDA, CIRRB as requested by the CIRRB Team Leader during an incident response.

12. Ensuring that compromised systems for which they are responsible remain disabled and/or disconnected from Forest Service's infrastructure, as directed by the USDA, CIRRB, until the ACIO for NRE or designate approves return to operational status.

13. Reviewing preventive and regular maintenance and maintenance logs and reporting any anomalies to the system owner.

14. Monitoring the use of hardware and software maintenance tools introduced to the information system specifically for diagnostic/repair actions and reporting any anomalies to the system owner.

15. Recognizing system security incidents or suspicious activities and immediately reporting them to the USDA, CIRRB.

16. Distributing copies of ISCPs to all those with a role or responsibility in executing them.

17. Using data from the Forest Service continuous monitoring tools to assess risk on an ongoing basis.

6683.04g - Information System Contingency Planning Coordinator

The Information System (IT) Contingency Planning Coordinator (CPC) is responsible for:

1. Supporting and participating, as required, in developing information system contingency plans (ISCPs).

2. Coordinating the testing, reviewing, and updating of the ISCPs, as necessary.

3. Assist in coordination of the training of all personnel with contingency responsibilities and verifying all have appropriate training and are trained periodically.

4. Assist in coordination of officials to establish teams and team leaders for damage assessment and recovery teams required to implement ISCPs.

6683.04h - Information System or Application Program Managers and Application Developers

The Information System/Application Program Managers and Application Developers are responsible for:

1. Performing configuration management during information system, component or service design, development, implementation, and operation.

2. Managing and controlling changes to the information system, component, or service.

3. Implementing only organization-approved changes.

4. Documenting approved changes to the information system, component, or service.

5. Tracking security flaws and flaw resolution within the system, component, or service.

6. Developing and implementing a plan for ongoing security and privacy control assessments.

7. Performing system, component or service testing/evaluation and produce evidence of testing and evaluation results.

8. Implementing a verifiable flaw remediation process.

9. Correcting flaws identified during testing and evaluation.

10. Following a plan to explicitly address security and privacy requirements.

11. Identifying the standards and tools used in the development process.

12. Documenting the specific tools and options and tool configurations used in the development process.

13. Documenting, managing, and ensuring the integrity of changes to the process and/or tools used in development.

14. Performing a criticality analysis when the architecture or design is modified or upgraded.

15. Reviewing the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options, and tool configurations selected can satisfy the security and privacy control requirements.

6683.04i - Information Technology Asset Managers

Managers of information resource assets are responsible for:

1. Tracking and documenting the issuance, replacement, and return of information technology (IT) equipment or resources and providing a copy of such documentation to users as part of the termination of personnel process.

2. Ensuring that Government-owned or provided IT equipment being returned or replaced during termination of personnel is returned to a pristine state before being reissued to another system user or being disposed of as excess property.

6683.04j - Information Technology Controlled or Restricted Space Employees

Employees assigned to work in information technology (IT) controlled or restricted spaces are responsible for:

1. Ensuring that any visitor is allowed access to IT restricted or controlled space only in accordance rules and regulations.

2. Challenging any unescorted individual in an IT restricted or controlled space not known to them, to have authorized access in that area.

6683.04k - Procurement and Property Services and Grants and Agreements

Forest Service Contracting Officers (COs), Contracting Officer's Representatives (CORs), Purchasing Agents and Grants Management Specialists are responsible for:

1. Ensuring that all IT-related contracts and agreements are reviewed and approved by ACISO or designate.

2. Ensuring that completed IT security training for cooperators and contractor personnel is properly documented in the USDA, AgLearn or other official Forest Service training documentation system.

6683.04l - Supervisors

Supervisors are responsible for:

1. Reporting, immediately, suspected or alleged IT related security violations, misconduct, or criminal activity to the Information System Security Officer or USDA, CIRRB.

2. Providing information and training to personnel in their units about operational security controls, limited personal use, and the appropriate use of information, information systems, and IT.

3. Ensuring that users under their supervision:

    a. Sign and renew, as required, any applicable access agreements, including non-disclosure agreements, before the access that requires the agreement is granted.

    b. Receive all security-related information and training required for information system users.

4. Determining the disposition of corporate information possessed or managed by departing users prior to their scheduled departure and assigning access of corporate information to other positions in the Forest Service.

5. Conducting exit interviews with departing users to establish that all:

    a. Corporate information under their management or control has been identified and properly turned over to the appropriate entity.

    b. Forest Service IT-related property in the user's custody has been returned to or accounted for by the appropriate entity, and the required transfer of custody procedures have been followed.

6. Ensuring that all information system media (both digital and non-digital) is considered for litigation hold and is sanitized according to the Forest Service policy and regulations before disposal or release for re-use.

7. Coordinating or assisting with the resolution of problems or issues affecting information system personnel screening.

8. Adding security and privacy roles and responsibilities into position descriptions.

6683.04m - Employees

All employees are responsible for:

1. Taking appropriate measures to protect information from unauthorized access.

2. Taking appropriate measures to protect computer equipment from theft, damage, or unauthorized use.

3. Reporting, immediately, suspected or alleged IT related security violations, misconduct, or criminal activity to their Supervisor or to the USDA, CIRRB.

4. Protecting passwords by not sharing or recording them in an unsecured location, and not permitting a browser or other application to save passwords.

5. Changing passwords within the timeframe required.

6. Signing off or electronically locking the computer before leaving it unattended.

7. Safeguarding their LincPass card and ensuring the LincPass is not left unattended in workstations when not in use.

8. Protecting sensitive information, including personally identifiable information, regardless of media.

9. Seeking out and applying appropriate security measures to protect sensitive information stored on the employee's computer.

10. Considering litigation hold before sanitizing all information system media (both digital and non-digital) according to the Forest Service policy and regulations, before disposal or release for re-use.

11. Signing any applicable access agreements, including non-disclosure agreements, before the access that requires the agreement is granted and renewing the agreements as required.

12. Ensuring that all Forest Service information and IT-related property is accounted for and transferred to an appropriate and authorized agency employee prior to termination from the Agency.

6683.04n - End Users

End users of Forest Service information systems are responsible for:

1. Understanding Forest Service IT security awareness requirements and completing required IT security training.

2. Backing up, or making available for backup, corporate information that they create or are otherwise responsible for, that are stored on a Forest Service laptop or desktop computer, smartphones, tablets, or other computing or information recording device by either:

    a. Storing copies of the information on assigned Forest Service file servers where it will be available for normal system backups, or

b. Storing copies of the information on Forest Service removable or external storage media and ensuring that the backup media are securely stored and protected according to the direction in this directive.

3. When connecting a Forest Service desktop or laptop computer to a home or public non-Forest Service network, ensuring that once network access is obtained the computer is immediately connected to the Forest Service Intranet via an approved VPN connection, and that all access to or through the public Internet using that computer occurs via that Forest Service VPN connection.

4. Ensuring that media containing sensitive information is protected from accidental or unintended disclosure.

5. Signing and renewing, as required, any applicable access agreements, including non-disclosure agreements, before the access that requires the agreement is granted.

6. Immediately reporting all computer/cyber security related incidents including but not limited to the loss, theft, or unauthorized access of any IT asset, or the suspected or alleged IT-related security violations, misconduct, or criminal activity; Immediately report compromise or suspected compromise in accordance with the USDA, CIRRB, procedures found on the CIO Cyber Security web page.

7. Ensuring that all Forest Service information and IT-related property is accounted for and transferred to an appropriate and authorized agency employee prior to termination from the Agency.

8. Considering litigation hold before sanitizing all information system media (both digital and non-digital) according to Forest Service policy and regulations before disposal or release for re-use. Protect and properly dispose of any and all media, including portable and removable devices that may contain sensitive information.

9. Not taking government devices (for example, computers, phones, tablets) when traveling outside the United States on personal travel.

10. Using only government devices (for example, computers, phones, tablets) specifically configured for international travel in accordance with current USDA and NRE Forest Service policy and procedures:

    a. when working outside the U.S while on official, approved international travel; or

    b. when working outside the U.S. under a telework agreement approved by both USDA and the Department of State.

6683.05 - Definitions [Reserved]

6683.06 - References [Reserved]

6683.07 - Team, Committee, and Group Responsibility [Reserved]

6683.1 - Media

6683.11 - Media Protection

6683.11a - Media Access

1. Information system media consists of all digital and non-digital media including backup media and removable Forest Service external storage devices.

2. Allow only authorized users to access information or information system media. Follow USDA guidance for the use of automated tools and capabilities to ensure levels of trust commensurate with the sensitivity of media before access is granted. [MP-2]

3. Utilize automated mechanisms to restrict access to media storage areas containing restricted media. Access attempts and access granted are audited.

4. Protect access to portable media (for example, USB drives, laptops, smart phones, tablets and personal electronic devices).

5. Use cryptographic mechanisms to protect and restrict access to information on portable digital media and devices and prevent unauthorized disclosure and modification of information at rest. [SC-28(1)]

6683.11b - Media Marking

1. Mark removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings as required. [MP-3]
2. All removable system media and information system output is exempt from security marking requirements as long as it remains within Forest Service controlled space. [MP-3]

6683.11c - Media Storage

1. Physically control and securely store IT system media. [MP-4]

2. Secure all digital and non-digital media that has sensitive information, including personally identifiable information (PII), in a locked cabinet, container, or drawer when not in use by authorized personnel. [MP-4]

3. Protect all media until the media is destroyed or sanitized using approved methods. [MP-4]

6683.11d - Media Transport

1. Protect all media during transport outside of controlled areas using appropriate security measures. [MP-5]

2. Implement appropriate physical and technical security measures for protection of media that are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. [MP-5]

3. Establish documentation requirements for activities associated with the transport of information system media in accordance with the assessment of risk. [MP-5]

4. Document, where appropriate, activities associated with the transport of information system media including accountability for media during transport outside of controlled areas. [MP-5]

5. Restrict the activities associated with transport of media to authorized personnel. [MP-5]

6683.11e - Media Sanitization and Disposal

1. Consider litigation hold guidance before sanitizing or disposing of media.

2. Sanitize all information system media (both electronic and paper) prior to disposal or release for re-use. [MP-6]

3. Use sanitization and disposal methods appropriate for the information's security categorization following guidelines found in National Institute of Standards and Technology (NIST) SP 800-88 Rev. 1 and Forest Service procedures. [MP-6]

6683.11f - Media Use

1. Prohibit the use of personally owned removable media in Forest Service information systems. [MP-7]

2. Prohibit the use of removable media in Forest Service information systems where the media has no identifiable owner. [MP-7]

3. Report loss, compromise, or suspected compromise of any media in accordance with the instructions found at the USDA CIRRB website.

6683.2 - Personnel Security

6683.21 - Separation of Duties

1. Separate work responsibilities to ensure that no individual acting alone can compromise the operational controls affecting the security and/or integrity of an information system or process.

2. In conjunction with HRM Personnel Security staff, conduct a risk assessment (RA) and assign position risk designations during initial information systems design and immediately following any design changes during the system's life. [PS-2] Identify the system's critical operational control functions, processes, and information. The RA must:

    a. Analyze position descriptions and temporary task assignments associated with critical operational control functions. Identify requirements for separation of duties and/or the need for compensating controls.

    b. Evaluate the effectiveness and appropriateness of the separation of duties and/or compensating controls specified in the personnel operating guidelines and procedures associated with the information system's critical operation control functions.

3. Support separation of duties, different individuals should perform each of the following actions for critical operational control functions: authorization/approval; system management; and monitoring or auditing.

    Examples of critical operational control functions include, but are not limited to:

    a. Should not be able to request an account and create one.

    b. Should not have the same account in the development and production environments. Change management, quality assurance, and testing processes implemented in information systems.

4. Maintain documentation of the implementation of separation of duties including any compensating controls.

5. Train all levels of the Forest Service IT System Management about the following principles of separation of duties:

a. No one individual should ever have all authority or access to information systems.

b. The activities of one group or individual should serve as a check on the activities of the other(s). Separating duties diminishes the likelihood that errors and wrongful acts would go undetected.

c. Separating duties limits the damages that could occur from errors or wrongful acts, particularly when used with RA, security training, and background investigations.

d. Always maintain documentation that proves there is a separation of duties.

e. Grant employees only the amount of access needed to perform their official duties.

6. Install and configure access control software on information systems and employ security capabilities to ensure users have the appropriate access to prevent users from performing fraudulent activities.

6683.22 - Position Risk Designation and Personnel Screening

Apply the following personnel screening requirements for use of Forest Service information systems in addition to any other criteria or requirements provided for by Forest Service policy or individual position determinations prior to authorizing access to any Forest Service information system. [PS-2]

1. Use the same personnel screening requirements for all users of Forest Service information systems regardless of employment status or relationship with the Forest Service.

2. Categorize and determine sensitivity (also known as a position risk designation) for all positions and assignments in accordance with HSPD-12 and approved Forest Service procedures. [PS-2]

    a. Classify positions at the sensitivity level commensurate with the highest level of information processed by the information systems that the occupant of that position will access.

    b. Include a statement of the need for contractor personnel screening, including HSPD-12 requirements, in all contracts, purchase orders, memoranda of understanding, memoranda of agreement, and other formal agreements or work order documents that will result in contractor access to Forest Service information and information systems.

3. Initiate required background investigations, through Personnel Security staff, in accordance with approved Forest Service procedures.

4. In the case of an emergency, such tasks may be assigned for a limited period to a person for whom the appropriate pre-appointment investigation has not been completed if a background investigation and request for advance fingerprint results has been initiated.

5. Conduct all personnel screenings, including initial and rescreenings, in accordance with Federal regulations and procedures such as 5 CFR Part 731.106; Office of Personnel, Management policy, regulations, and guidance; FIPS 201 and SPs 800-73, 800-76, 800-78, HSPD-12 requirements, and Forest Service procedures; and the criteria established for the risk designation of the assigned position. [PS-3]

6. Review and update position risk designations as required. [PS-2]

7. Develop and implement rescreening procedures according to position-defined rescreening frequency and criteria. [PS-3]

6683.23 - Personnel Hiring, Transfer, and Separation

6683.23a - Personnel Hiring and Information Security Awareness

For all new or newly assigned Forest Service employees, volunteers, partners, cooperators, contractor employees, and others who will require access to Forest Service information technology (IT) facilities and use of Forest Service information systems and IT equipment:

1. Provide required information security awareness training with rules of behavior and appropriate use of Forest Service information systems and equipment prior to granting access to any Forest Service information system. [AT-2]

2. Provide information security awareness refresher training for all personnel requiring access to Forest Service IT systems. [AT-2]

3. Provide additional role-based security and privacy training to personnel with assigned security and privacy roles and responsibilities and incorporate security and privacy roles and responsibilities into their position descriptions. [PS-9, AT-3]

6683.23b - Personnel Termination

For any Forest Service user being suspended or whose employment is voluntarily terminated: [PS-4]

1. Immediately notify Human Resources Management, Customer Help Desk and the appropriate management of the user's departure date to ensure that all access to facilities and systems are terminated.

2. Deactivate all user accounts and access rights (network, applications, e-mail, voice, physical access, authenticators, and credentials) no later than close of business on the next business day following the date of departure.

3. Retrieve all Government IT equipment, software, files, keys, and badges issued to the employee, document the retrieval, and provide the user a copy of that documentation.

4. Conduct, in conjunction with Personnel Security staff, an exit interview with the departing system user to obtain any security related information that may not be available or apparent in existing documentation and reiterate the continued obligations under the IT non-disclosure, confidentiality, or user access agreements.

5. Reassign access of organizational information and systems to other positions within the Forest Service. [PS-4]

For any Forest Service user whose employment is involuntarily terminated [PS-4]:

1. As appropriate, notify Human Resources Management, the CIO staff, the Contracting Officer, the ISSO, LEI, Personnel Security staff, and the Facility Manager of the user's departure date to ensure that all access to facilities and systems are terminated.

2. For personnel or contracting actions resulting in the separation of the user, deactivate all accounts and restrict physical access to information resources, personnel, and facilities at the time the user is notified of the action or requested by LEI or the user's Supervisor when risk of damage to IT resources warrants immediate action.

    a. Prior to departure, determine the disposition of electronic and printed files owned or managed by the departing employee and that contain corporate information, except as follows:

        (1) If the user is under investigation for suspected inappropriate use of Government information systems, leave such files intact.

        (2) If the disposition of files cannot be determined prior to departure, move them to a secure location for later determination.

b. Retrieve all Government IT equipment, software, files, keys, and badges issued to the user, document the retrieval, and provide the user a copy of that documentation.

3. Reassign access of organizational information and systems to other positions within the Forest Service. [PS-4]

6683.23c - Personnel Transfer

When personnel are reassigned or transferred:

1. Follow personnel transfer procedures to properly schedule the transfer and initiate the necessary changes of information system accounts and access privileges.

2. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions with the Forest Service. [PS-5]

3. Reissue keys, identification cards, building passes; close old accounts and establish new accounts; and change system and facility access authorizations where appropriate and notify appropriate personnel when completed. [PS-5]

6683.23d - Long-term Absence

If an information system user will be on extended leave or other long-term absence, such as seasonal employment or a special assignment (detail):

1. Disable access for that user from information systems, IT equipment, and facilities to which they will not require access during their absence. Allow continued use by the user of a particular information system during the absence only when a need for continued access has been identified to and approved by that system's owner and Supervisor.

2. Do not delete accounts if it is understood that the user will be returning to employment with the Forest Service and/or their assigned unit.

3. Require the user to appropriately secure any sensitive or potentially sensitive information from computers or other IT equipment they will be leaving behind during their absence.

4. Reassign the user's equipment or allow use by others only when it has been determined that such shared use will not create additional security risks.

6683.23e - Access Agreements

Before granting access or providing equipment, the Forest Service: [PS-6]

1. Ensures that individuals take and pass the USDA security awareness training and accepts the Rules of Behavior.

2. Develops access agreements needed for the system.

3. Executes access agreements, including a Non-Disclosure Agreement (NDA) if a non-disclosure agreement is needed from contractors or cooperators before granting access to Forest Service information.

4. Reviews these access agreements and rules of behavior as required. [PS-6]

6683.23f - External Personnel Security

1. Include explicit personnel security requirements in all acquisition related documents such as statement of work, request for proposals, and so forth. [PS-7]

2. Require contractors and other external service providers to comply with requirements set forth by Forest Service policy and procedures. [PS-7]

3. Subject contractors and other external service providers to the same personnel screening requirements as Forest Service personnel. The IT system owner may coordinate with the Contracting Officer to tailor the appropriate personnel screening level for contractors or external personnel in alignment with the risk level of the information system and the contractor’s planned access roles or responsibilities. [PS-7]

4. Require contractors and other external service providers to formally certify that they will notify the Forest Service's Procurement and Property Services and CIO Office upon the termination or departure of any of their contract employees and accept responsibility for the return of all Government-owned or -furnished equipment, such as keys, tokens, or identification badges. [PS-7]

5. Monitor external personnel security compliance. [PS-7]

6. Provide a Forest Service desktop or laptop computer to all contractors or external personnel that need system access to the Forest Service network.

    a. Ensure that once network access is obtained the computer is immediately connected to the Forest Service Intranet via an approved VPN connection, and that all access to or through the public Internet using that computer occurs via that Forest Service VPN connection.

b. Ensure that no Forest Service VPN software is installed on non-government computers.

7. Ensure all Government-provided laptop computers are running USDA approved Disk Encryption software, the latest Forest Service corporate software and security patches. [AC-19(5)]

6683.23g - Physical Safeguards of Forest Service-owned or Forest Service-leased IT Equipment

When using Forest Service-owned or -leased IT equipment, Forest Service personnel will:

1. Exercise due care to protect Forest Service-owned or -leased IT equipment from the introduction of food, beverages, cigarette ashes, paper clips, staples, or other hazards.

2. Physically secure laptop and notebook computers when left unattended, whether docked or undocked.

3. Engage the screen lock whenever any computer is left unattended.

4. Protect all personal computers from extreme environmental conditions, such as extreme dust and dirt from construction or outdoor exposure, or extreme heat, cold or moisture.

5. When traveling:

    a. Keep laptops in carry-on luggage and make every reasonable effort to keep laptops and other IT equipment assigned to the employee in sight during security screening at security checkpoints.

    b. Except for security checkpoints, never entrust laptop and notebook computers, however briefly, to anyone who is not working with the Forest Service in some capacity. Only employees, contractors, or others working on behalf of the Forest Service should be granted even temporary custody of Forest Service equipment.

    c. Exercise due diligence in securing and/or concealing laptops when staying in hotels to protect them, based on the employee's assessment of the risk at the particular location.

    d. Do not leave laptops in hotel baggage hold rooms, unless reasonably assured of the safety of the equipment.

    e. Attach identification to laptops.

f. End users are prohibited from taking government computers/phones/tablets when traveling outside the United States on personal travel.

g. For approved, official travel outside of the United States, use only government devices (for example, computers, phones, tablets) specifically configured for international travel. Upon return the device may need to be reimaged in accordance with USDA and Forest Service policy and procedures prior to connecting to the network to eliminate any malicious code.

h. Prior to departing the United States for either official travel or approved overseas telework, refer to current USDA and NRE Forest Service policies and procedures to obtain approval for using devices and securing remote access to USDA information and information systems.

6. Immediately report the loss, theft, or destruction of any IT asset or information to the USDA, CIRRB.

7. Immediately report loss or theft of servers, laptops, desktop computers, or other hardware devices or media containing Forest Service information to both LEI and Supervisor following home unit procedures. When on travel, also report such loss or theft to local police, and if possible, obtain a copy of the police report and furnish it with the report to USDA CIRRB, LEI, and Supervisor.

6683.24 - Appropriate Use of Information Technology Resources

This section provides direction on the appropriate use of Forest Service-owned or -leased IT resources.

1. This direction in no way limits Forest Service personnel in the use of Forest Service IT for official and authorized activities.

2. If some job function seems to be hampered by this policy, personnel should contact their Supervisor or COR for assistance.

3. Hereafter, the terms “employee,” “employees,” “user,” and “personnel” refer to all who use Forest Service-owned or -leased information resources.

4. In some instances, emergency incident operations may be granted waivers to some provisions of the direction in this section related to operational security controls.

5. Collaborative computing devices, such as webcams, video and audio-conferencing devices, may not be activated remotely except where Forest Service or USDA policy creates exceptions allowing remote activation. Local or remote activation of collaborative computing devices must provide an explicit indication of use to individuals physically present at the devices. Exceptions to the prohibition against

remote activation of collaborative devices must conform to Forest Service and USDA policy and must be defined in the System Security Plan (SSP) of the affected information system. [SC-15]

6. Do not access Forest Service information systems, other than those that are publicly available, using personally owned equipment unless authorized to do so.

7. Although the direction in this section focuses primarily on computers, the direction also applies to other electronic, telecommunications, and information resources, technology, services, and devices.

8. The system will provide an explicit indication of use to individuals physically present at the devices.

6683.24a - Limited Personal Use

1. Department Regulation (DR) 3300-1 and the policy for "Limited Personal Use of Telecommunication Resources and Office Equipment" negotiated between the Forest Service and the Forest Service Partnership Council authorize limited personal use of Government telecommunications resources and equipment by employees in the workplace on an occasional basis, provided that the use involves minimal expense to the Government and does not interfere with official business.

2. DR 3300-001 covers Forest Service telecommunications equipment (for example, mobile devices, tablets, computers, local area network, telephones, printers, facsimile equipment) and services (for example, electronic messaging services and systems, Internet, Forest Service Intranet and file sharing sites, and social media).

3. Employees may use Forest Service IT resources for non-Forest Service purposes when such use involves minimal additional expense to the Forest Service, is normally performed on the employee's non-work time, does not interfere with the mission or operations of the Forest Service, and does not violate the Standards of Ethical Conduct for Federal employees.

6683.24b - Proper Representation

When using Forest Service equipment for non-Forest Service purposes, employees shall ensure it is clear they are acting in a personal, and not an official, capacity. If there is a possibility that such a personal use could be interpreted as representing the Forest Service, then an adequate disclaimer must be used.

6683.24c - Inappropriate Personal Uses

All personnel are expected to conduct themselves professionally in the workplace and to refrain from using Forest Service telecommunications and information technology (IT) resources for inappropriate activities. Inappropriate activities include, but are not limited to the following:

1. Illegal activity, such as, but not limited to, copyright violations, unauthorized access to Forest Service or other systems, possession or transmittal of child pornography, use of Forest Service computer systems to facilitate a crime, or assistance to others in gaining unauthorized access to Forest Service or other systems.

2. Use of Forest Service telecommunications and IT resources for activities that are inappropriate or offensive to fellow employees or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

3. The creation, copying, transmission, or retransmission of chain letters or other unauthorized mass mailings, regardless of the subject matter (for example, sending to lists of multiple unknown recipients where no official business relationship exists). This is also known as “spam.”

4. The creation, download, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials.

5. The creation, download, viewing, storage, copying, or transmission of materials related to gambling.

6. Posting of Forest Service information to external news groups, bulletin boards, or other public forums without authorization. This includes any use that could create the perception that the communication was made in one's official capacity as a Forest Service employee (unless appropriate Forest Service approval has been obtained).

7. Destruction or modification of Government information except in the course of executing assigned duties or with authorization.

8. Intentional introduction of malicious software (viruses or worms) or infected files onto Government equipment.

9. Any personal use that could cause congestion, delay, or disruption of service to any Forest Service system or equipment, such as, but not limited, to large file attachments, “streaming” technology such as stock or news tickers, continuous sports feeds, Internet radio, or administration of non-Forest Service websites.

10. Any use that could generate more than minimal additional expense to the Forest Service, such as frequent or lengthy personal local phone calls or faxes, or more than occasional use of a copier to make one or two personal copies.

11. Commercial purposes in support of "for-profit" activities or in support of other outside employment or business activity, such as consulting for pay, sales or administration of business transactions, sale of goods or services, or website administration.

12. Engagement in any outside fundraising activity, endorsement of any product or service, participation in any lobbying activity (except for activities permitted under the Hatch Act and Article 5 of the Master Agreement between USDA Forest Service and the National Federation of Federal Employees), or engagement in any prohibited partisan political activity.

13. Installation or use of unauthorized software, including personally owned software, on Government equipment.

14. Use of Forest Service equipment to administer non-business-related personal mailing lists.

15. Use of the Forest Service network as a substitute for obtaining an Internet service provider for home Internet access.

16. Automated forwarding of Forest Service e-mail to a non-Forest Service domain e-mail account (because all Forest Service work is considered “official business” and as such should not be forwarded to a personal e-mail account).

6683.24d - Peer-to-Peer Networking, Networked Collaboration Tools, and Instant Messaging

1. Forest Service employees are prohibited from installation and use of any peer-to-peer networking, networked collaboration, or instant messaging tools, other than the Forest Service’s authorized enterprise remote access, file transfer, collaboration, or instant messaging tools.

2. Do not install or use on any Forest Service system any unauthorized peer-to-peer or instant messaging software.

3. Re-imaging is required when such unauthorized peer-to-peer networking or instant messaging software as described in the preceding paragraph is found on a computer.

4. Any Forest Service machine that does not have the Forest Service image installed (such as various point solution servers and computers that are not a part of the

Forest Service computer base) on which unauthorized peer-to-peer networking software is found must be reloaded immediately from pristine media.

5. Forest Service boundary network devices must be configured to block the communication ports associated with these prohibited protocols.

6. Control and document the use of allowed enterprise peer-to-peer networking, network collaboration, and instant messaging tools to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.

6683.24e - Unauthorized Access

1. Forest Service personnel utilizing Forest Service-owned or -leased information resources shall access Forest Service networks or equipment only via authorized connection through the Forest Service network. [AC-17(2)]

2. Access through unauthorized use of remote-control software that permits access to Forest Service equipment from outside the Forest Service network is prohibited unless technical approval has been obtained for installation of such software. [AC-17(10)]

6683.24f - Elevated Privileges

1. When an employee's privileges are temporarily elevated to permit installation of nonstandard but authorized software, install only software that has been approved for installation.

2. Do not use access to an account with administrative privileges to elevate the rights on personal accounts or to perform any other activity that is not specifically authorized.

6683.24g - Software Usage Restrictions

1. All software installed on Forest Service computer equipment that is not part of the Forest Service image must be authorized for use within the Forest Service computing environment. Authorization for software not contained in the image may be obtained either via the pre-approved software list or the Technical Approval Process. [CM-10]

2. Unless explicitly authorized for execution of authorized job-related functions, users shall not install software intended to identify or exploit IT vulnerabilities.

3. Employees shall not:

a. Download or install patches of any kind to standard corporate software without authorization.

b. Install add-ins or plug-ins.

c. Install unauthorized freeware or shareware.

d. Install, download, or run prohibited software.

4. Employees shall keep security patches installed and up to date on all commercial off-the-shelf software, provided the original software installation was approved.

5. The Forest Service will enforce authorized software compliance using Agency-specified monitoring tools. [CM-11]

6. The Forest Service will monitor compliance at USDA-defined intervals. [CM-11]

7. Employees shall not use unlicensed software or copy licensed software for use on systems other than those for which it was approved for use.

8. Software and associated documentation must be used in accordance with contract agreements and all applicable intellectual property laws, such as copyright. [CM-10]

9. Tracking systems must be employed for software and associated documentation protected by quantity licenses to control copying and distribution [CM-10].

10. The use of peer-to-peer file sharing technology must be controlled and documented to ensure that this capability is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work. [CM-10]

6683.24h - Privacy Expectations

By using Forest Service IT equipment, employee consent is implied for the following:

1. Monitoring and recording of activities as necessary to ensure the smooth, reliable performance and secure operation of information systems as required by law and in accordance with Article 4 of the Master Agreement between the USDA, Forest Service and National Federation of Federal Employees, including, but not limited to, monitoring and recording of Internet access and e-mail transmissions or receipts.

2. Disclosure of the contents of any files or information maintained on or passed through Forest Service IT resources to employees who have a need to know in the performance of their duties. Forest Service officials, such as system Managers and Supervisors, may access any electronic communications as necessary to maintain

reliable and secure information system operation or to investigate reports or indications of improper use.

3. The understanding that any use of Forest Service communications resources generally is not secure, is not private, and is not anonymous, and that system Managers do employ monitoring tools to detect improper use. There is no right to privacy when using Government information systems.

4. The potential for investigation of files stored on an employee's computer for reasons unrelated to the employee. Although Supervisors shall not investigate files stored on an employee's computer without cause, employees should be aware that circumstances external to the employee can generate such a cause. The course of a security incident investigation, for example, may require that all computers in a specific unit be searched, thus possibly exposing personal files to management scrutiny.

6683.24i - Personnel Sanctions

1. Each suspected incident of unauthorized or improper use of Forest Service equipment, failure to take prudent physical security measures to protect Forest Service equipment, or other noncompliance with Forest Service information security policies and procedures, will be investigated. [PS-8]

2. Findings of culpability will result in disciplinary action, which may include the employee's loss of use or limitations on use of equipment, disciplinary or adverse action, criminal penalties, and/or financial liability for the cost of improper use. [PS-8]

3. Notify Supervisor when a formal sanction process is initiated, identifying the individual sanctioned, and the reason for sanction. [PS-8]

6683.3 - Physical and Environmental Protection

6683.31 - Physical Access Authorizations

1. Review, approve, and update the access authorization list as required. If a user's access is no longer warranted, or if that user is no longer with the Forest Service, remove that user's access privileges immediately. [PE-2]

2. Issue an authorization credential (security badge or other personal identity verification (PIV) device) to each person allowed unescorted access to Forest Service's IT controlled or restricted space or facilities. [PE-2]

3. The information system accepts and electronically verifies PIV credentials from other Federal agencies for personnel that have authorized access to the system where possible. [IA-2(12), IA-8(1)]

4. PIV devices must:

    a. Be worn or attached at or above the waistline of the individual so as to be visible at all times when viewing the individual from the front.

    b. Conform to the requirements of Homeland Security Presidential Directive 12 (HSPD-12).

    c. Clearly indicate if the wearer is a Forest Service employee, contractor, or authorized visitor.

5. Document and report security violations or suspicious activity to the USDA, CIRRB. [PE-6]

    a. In the event of unauthorized access to an IT facility, contact the proper enforcement officials, and ensure that the individual is escorted from the facilities.

    b. Document all incidents and take appropriate action according to security policies.

6. Permit uniformed and/or credentialed law enforcement, fire, or emergency medical services personnel responding to an emergency call to deviate from any part of the requirements in this chapter that inhibit their emergency response efforts.

6683.32 - Physical Access Control

1. For access to areas containing information systems or network components, consider all individuals without permanent authorization credentials to be visitors and: [PE-3]

    a. Document their visit.

    b. For an IT restricted space, issue temporary identifications (IDs) for the duration of their visit.

    c. Verify that all visitors have a legitimate reason to enter information technology (IT) restricted or controlled space before allowing access.

    d. Escort visitors and monitor visitor activity when required. [PE-3]

2. Require visitors to sign a log upon entering IT restricted or controlled spaces and sign out upon exiting. The log must minimize PII and record the visitor's name, organization, purpose of visit, and identity of escort or person/office being visited, as appropriate.
   [PE-3,8, 8(3) PRIV]

   a. Review the visitor access logs as required. [PE-6,8]

   b. Retain the logs or in accordance with official records management and retention requirements. [PE-8]

3. Designate and control access to areas officially designated as publicly accessible in accordance with the facility's assessment of risk. [PE-3]

4. Define and document the security safeguards used to control access to areas within facilities officially designated as publicly accessible.

5. Monitor physical access to the information system to detect and respond to physical security incidents.

6. Provide real-time physical intrusion alarms and surveillance equipment for IT controlled or IT restricted space. [PE-3]

7. Utilize real-time physical intrusion alarms and surveillance equipment where practical. [PE-3]

8. Conduct inventories of all physical access devices as required. [PE-3]

9. Re-key or change the combinations of high security locks when the keys and/or combinations are lost or compromised, or when individuals in possession of the keys or combinations are transferred or terminated. [PE-3]

10. Promptly disable access authorizations of PIV or other electronic access mechanisms when the access device is reported lost or stolen, or when the individual is transferred or terminated.

6683.33 - Information Technology Facilities

1. Physically secure all Forest Service information technology (IT) facilities commensurate with their importance to the ability of the Forest Service to accomplish its mission, excluding those areas within the facility that are officially designated as publicly accessible. Locate IT equipment in locked rooms or enclosures secure enough to appropriately mitigate the risk of unauthorized physical access, at a minimum.

2. Incorporate physical security requirements into all plans and designs for new or remodeled IT space or facilities.

3. Test environmental protection devices or systems to ensure they are operating and will function as intended, periodically.

4. Protect power equipment and power cabling for information systems from damage and destruction. [PE-9]

5. Regulate temperature and humidity in facilities housing Forest Service IT components. [PE-14]

6. Monitor temperature and humidity levels continuously. [PE-14]

7. Protect Forest Service IT equipment from potential water damage. Master shutoff valves must be provided that are accessible, working properly, and known to key personnel. [PE-15].

8. Implement and assess the effectiveness of all applicable NIST- and USDA-compliant security controls, including but not limited to management, operational, and technical controls at all Forest Service alternate work sites. Notify Supervisor in the event of an incident at alternate work site. [PE-17]

9. Locate medium and output devices which display sensitive information or PII in the interior of the building away from exterior windows and positioned so as not to be visible from passersby. [PE-5]

10. Position information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access. [PE-16]

11. For controlled access areas, shut doors and ensure windows are screened to prevent unauthorized viewing of the monitor. [PE-5]

12. Implement an emergency shutoff process and capability. Ensure that emergency shutoff switches or devices are located to facilitate safe and easy access for personnel and are protected from unauthorized activation. [PE-10]

13. Provide emergency backup power sufficient to maintain automatic emergency lighting for facility interior and entrances/exits as specified in the local emergency evacuation plan. [PE-11]

14. For IT controlled space:

a. Locate space in the interior of the building away from exterior windows to the extent possible.

b. Secure IT equipment in a locked room, closet, or in locking cabinets with tamperproof hinges.

c. Do not identify equipment locations in building directories or on orientation floor plans accessible by visitors or the general public. If lockers, cabinets, or entrances to rooms or closets housing IT equipment must be located in publicly accessible areas, do not apply external markings indicating their function.

d. Provide appropriate detection of and protection from fire that activate automatically and notify emergency responders when the facility is both staffed and unstaffed. Fire detection and suppression devices/systems must be supported by an independent energy source and deployed in accordance with local fire codes.

e. Provide uninterruptible power supply or equivalent emergency backup power systems if warranted by the nature of the components in the space.

f. Ensure that the environment provides temperature and humidity control sufficient to meet manufacturer operating parameters for the IT equipment contained in the space.

g. Implement access controls that:

(1) Provide an audit trail of all physical access to the space and/or equipment.

(2) Prevent access by unauthorized individuals.

15. For IT restricted space:

a. Meet the physical security requirements for IT controlled space (see previous paragraphs).

b. Provide well-lit, controlled parking areas, including arrangements for removal of unauthorized vehicles.

c. Monitor and control access to the facility at all times using security guards and intrusion detection systems with central monitoring capability maintained to current life safety standards. [PE-6(1)]

d. Equip all IT restricted space entrances/exits with high security locks inspected as required by IT personnel.

e. Re-key or change the combinations of high security locks as required, or when the keys and/or combinations are lost or compromised, or when individuals in possession of the keys or combinations are transferred or terminated.

f. Maintain a current inventory of these high security locks and secure all keys and combinations and other access devices.

g. Provide surveillance cameras with time-lapse recording capability at all entrances and exits.

h. Provide lighting with emergency backup at all IT restricted space perimeter entrances/exits and between facility entrances/exits and IT restricted spaces. [PE-12]

i. Require security guards or equivalent personnel to X-ray or otherwise inspect all packages not mailed or shipped from a trusted source before delivery within the facility. Log all deliveries.

j. Locate the space in the interior of the building away from exterior windows, and not directly above or below visitor activity areas, mailrooms, or loading docks, to the extent possible.

k. Protect the space using an automatic fire suppressant system in accordance with local fire codes, preferably dry pipe. Test and monitor all fire suppression and prevention devices and immediately replace defective devices. [PE-13, 13(1)]

l. Provide only the minimum number of entrances/exits allowed by local fire codes and use metal or solid wood doors with at least a 2-hour fire rating and tamperproof hinges. Do not use glass doors or windows.

m. Enclose the space with hard walls extending from the fixed floor to the fixed ceiling. Do not terminate perimeter walls at the surface of a floating (raised) floor or hanging ceiling.

n. Use an electronic, preferably biometric, control for access to IT restricted space that provides an audit trail, is removed from any master key systems for the facility and includes a centrally monitored intrusion detection system active on all IT restricted space perimeter entrances and exits. [PE-2]

o. Provide the space with automatic emergency backup power sufficient to: [PE-11]

(1) Maintain physical access controls and emergency interior lighting during power outages.

(2) Maintain server, information/voice/video/radio or other communications, and heating/ventilation/air conditioning (HVAC) operations during a power outage in accordance with the system security plan or operation guide for the systems involved, but at a level at least sufficient to accomplish an orderly shutdown of all equipment within the space

p. Provide the space with temperature control, using redundant HVAC systems, if necessary, sufficient to: [PE-14]

(1) Keep all equipment operating within manufacturer recommended temperature ranges during normal operation, and

(2) Keep equipment within the space that is designated as mission-critical in its system security plan operating within manufacturer recommended temperature ranges during a failure of either the primary IT restricted space HVAC system or one of the redundant HVAC systems, if installed.

q. Include those requirements and specifications in all leases or contracts for IT restricted space, including contracts for design and construction of such spaces.

16. Control physical access to information system distribution and transmission lines within Forest Service facilities. [PE-4]

6683.34 - Delivery and Removal of IT Related Items

1. Authorize and control all designated information system components (for example, hardware, firmware, software) entering or exiting information technology (IT) restricted space. [PE-16]

2. Items may be authorized by designated officials or system owners only.

3. Maintain records of those items entering and exiting IT restricted space including the information system to which the items are assigned, and the final location where these items will reside. [PE-16]

4. Maintain appropriate records of such items, including delivery logs.

5. Control access to loading docks and other delivery or receiving/shipping areas and isolate such areas from the information system and media libraries to reduce the risk of unauthorized physical access. [PE-16]

6683.4 - Information System Contingency Planning

1. Establish a Forest Service-wide information system contingency planning process and incorporate contingency planning into the System Development Life Cycle (SDLC) for all information systems. [CP-1]

2. Identify and prioritize critical IT resources for emergency response and recovery and determine the minimum actions necessary to restore mission critical core business functions. [CP-2(8)]

3. Identify preventive measures that could be taken to reduce the effects of information system disruptions. [CP-2]

4. For all major information systems, develop and implement ISCPs that: [CP-2]

    a. Identify essential missions and business functions and associated contingency requirements.

    b. Provide recovery objectives, restoration priorities, and metrics.

    c. Provide clear and specific activation criteria.

    d. Provide clear, understandable, sufficiently detailed guidance to allow orderly and efficient restoration and reconstitution of disrupted information systems and the business functions they support.

    e. Include recovery and reconstitution strategies to ensure disrupted systems can be reconstituted and recovered quickly and effectively following an incident. [CP-2(3)]

    f. Clearly assign individual responsibilities, roles, and authorities with associated lines of succession for response and recovery efforts and contact information.

    g. Identify resources or facilities that must be arranged in advance to ensure ISCPs can be executed.

    h. Define communication procedures and priorities to be used during an emergency or crisis, including key contacts.

    i. Are approved by the principal parties affected by or involved with the plan.

j. Address contingency roles, responsibilities, and assigned individuals with contact information.

k. Address maintaining essential mission and business functions despite an information system disruption.

l. Address eventual, full information system restoration without deterioration of security safeguards originally planned and implemented.

5. Review ISCPs and update as necessary. [CP-2]

6. Coordinate ISCP development with Forest Service elements responsible for related plans listed in exhibit 01, Types of Contingency Plans. [CP-2(1)]

7. Define the specific types of teams and assign individuals to these teams that will be needed for implementing the ISCP based on the systems affected. [CP-2]

8. Distribute updates and make available copies of ISCPs to all those with a role or responsibility in executing them. The key personnel are to be defined in the information system ISCP. [CP-2]

9. Coordinate related ISCPs to avoid conflict or duplication of effort. [CP-2]

10. Protect the ISCPs from unauthorized disclosure and modification. [CP-2]

6683.4 - Exhibit 01

Types of Contingency Plans

Contingency Plan	Purpose	Function
Information System Contingency Plan (ISCP)	Recover IT (broad range of disruptions)	Provides guidance for recovering specific IT functionality or specific information systems.
Continuity of Operations Plan (COOP)	Sustain National and Regional Headquarters	Focuses on restoring essential functions at an alternate site.
Critical Infrastructure Plan	Sustain/Recover national assets relating to the safety, security, economy, and/or health.	Focuses on policies and procedures for compliance with the HSPD-7 risk management framework for the nation's critical infrastructure and key resources.
Business Continuity Plan (BCP)	Sustain/Recover Business	Focuses on sustaining business processes during and after a disruption.
Disaster Recovery Plan (DRP)	Recover IT (major disruption)	Applies to major events that deny access to a facility for an extended period of time.
Cyber Incident Response Plan	Recover IT (malicious attack)	Establishes procedures to address cyber-attacks against information systems.
Crisis Communications Plan	Communications	Establishes internal and external communications procedures.
Occupant Emergency Plan (OEP)	Personnel Safety	Provides the response procedures for occupants in the event of a situation requiring evacuation or shelter-in-place.

6683.41- Continuity of Operations Plan

1. Develop a Continuity of Operations Plan (COOP) for Forest Service Agency headquarters, Regional Offices, and Research Station headquarters that provides for the restoration of mission essential and critical functions at an alternate site following a disaster, or other events that makes the primary site unusable.

2. Identify in the COOP those IT requirements necessary to support the primary function, such as emergency communications, authorities, and establishment of the chain of command.

3. Identify in the COOP those critical information system assets supporting essential missions and business functions. Supporting information can be found in the system Business Impact Analysis. [CP-2(8)]

4. Design the plan to take maximum advantage of existing Forest Service IT infrastructures.

5. Coordinate COOP development with Forest Service elements responsible for related plans, such as those listed in section FSM 6683.4, exhibit 01, Types of Contingency Plans. [CP-2(1)]

6. Review and test the COOP IT components as required to ensure that the IT functions operate as planned. Make updates to the COOP as necessary based on results of this review and testing.

7. Arrange in advance, through solicitations, contracts, and agreements, for the use of the alternate sites, facilities, or other resources required by the COOP. Ensure these agreements are readily accessible to COOP personnel.

8. Design and implement protocols to protect the COOP from unauthorized disclosure and modification, and document them in the COOP.

6683.42 - Contingency Training

1. Provide training to all personnel with contingency roles and responsibilities with respect to the information systems of their assignment to this role. [CP-3]

2. Ensure that training results in participants' understanding of both the applicable contingency plans and their roles defined within the plans. [CP-3]

3. Provide refresher training when required by information systems changes and at regular intervals as required. [CP-3]

6683.43 - Contingency Plan Testing

1. Unless otherwise specified below, test ISCPs for information systems at regular intervals or after significant system changes to determine the effectiveness of the plan and the organizational readiness to execute the plan. [CP-4]

2. Test or exercise ISCPs for mission essential and critical (including financial) systems or after significant system changes to ensure the plans are executable. [CP-4]

3. Conduct tests using Forest Service-defined tests and/or exercises (tabletop for low systems and functional for moderate and high systems) in order to determine the plan's effectiveness and the Agency's readiness to execute the plan. [CP-4]

4. Review ISCPs test/exercise results and initiate corrective actions to include correcting any deficiencies found during testing. [CP-4]

5. Coordinate ISCP testing with other Forest Service elements with responsibilities in related plans such as a Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, and Emergency Action Plan. [CP-4(1)]

6683.43a - Continuity of Operations Plan Testing Requirements

1. Review and test the Continuity of Operations Plan (COOP) on an annual basis or after a significant organizational change, to ensure that it: [CP-4]

    a. Can be executed with or without warning.

    b. Will protect essential assets and provide continuous operation of essential functions.

2. Arrange in advance, through solicitations, contracts, and agreements, for the use of the alternate sites, facilities, or other resources required by the COOP. [CP-6]

3. Review the testing results and initiate corrective action, if necessary. [CP-4]

6683.43b - Business Resumption Plan Testing Requirements

1. Review and test, at least as a tabletop exercise, each Business Resumption Plan (BRP) to ensure that it can be executed and that it will, in fact, restore normal business operations as intended.

2. Review the testing results and initiate corrective action, if necessary.

6683.43c - Backup and Recovery Plan Testing Requirements

1. Test recovery procedures as required. The test must include full system and/or database restoration from backup media.

2. Review the testing results and initiate corrective action, if necessary.

6683.44 - Alternate Storage Sites

1. Establish an alternate storage site and initiate necessary agreements to permit the storage of systems backup information, appropriate to system categorization. [CP-6]

2. Ensure that the frequency of information systems backups and the transfer rate of backup information to the alternate storage site (if so designated) are consistent with the Forest Service's recovery point objectives. [CP-6]

3. Ensure that the alternate storage site is geographically separated from the primary storage site as not to be susceptible to the same hazards identified at the primary storage site and is not likely to be affected by the same event that rendered the primary storage site backup media unavailable. [CP-6(1)]

4. Ensure that the Forest Service identifies potential accessibility problems to the alternate storage site in the event of an area wide disruption or disaster and outlines explicit mitigation actions. [CP-6(3)]

5. Ensure that the alternate storage site provides a level of security and protection no less stringent than provided for the primary site and has a safe environment providing temperature and humidity regulation, water damage protection, fire prevention, and power management controls. [CP-6]

6. Ensure that the alternate storage site protects the confidentiality and integrity of the backup information at the alternate storage site. [CP-6]

6683.45 - Alternate Processing Sites

1. Appropriate to system categorization, establish an alternate processing site and initiate necessary agreements to permit and support the organization-defined time period for the resumption of information systems, in accordance with the system's ISCP, when the primary processing capabilities are unavailable. [CP-7].

2. Make available equipment and supplies required to resume operations in accordance with the system's ISCP. [CP-7]

3. Develop a Memorandum of Understanding/Agreement (MOU/A) or a service level agreement specific to the organization's needs. [CP-7]

4. Establish contracts as required to support Forest Service established recovery time objectives. [CP-7]

5. Ensure that the alternate processing site is geographically separated from the primary processing site so as not to be susceptible to the same hazards as identified at the primary processing site. [CP-7(1)]

6. Ensure that the Forest Service identifies potential accessibility problems to the alternate processing site in the event of an area wide disruption or disaster and outlines explicit mitigation actions. [CP-7(2)]

7. Ensure that the alternate processing site agreements contain priority-of-service provisions in accordance with availability requirements. [CP-7(3)]

8. Ensure backup copies of ISCPs are available at alternate processing locations.

9. Ensure that the alternate processing site provides information security measures no less stringent than those of the primary site. [CP-7]

6683.46 - Telecommunications Services

1. Establish primary and alternate telecommunications services to support information systems and initiates necessary agreements with priority -of-service provisions to permit the resumption of those information systems' operations as defined in the ISCP.
   [CP-8, 8(1)]

2. Ensure that alternate communications services do not share a single point of failure with the primary telecommunications services. [CP-8(2)]

6683.47 - System Backup

1. Back up Forest Service corporate data and information systems in a regular scheduled way using cryptographic mechanisms that enables information or system recovery within a time period dictated by the relevant SSP; applicable ISCPs; and in accordance with applicable policies, regulations, or service level agreements. This includes user-level data, system-level data, system-state information, information system documentation, operating system and application software. [CP-9, 9(8)]

2. Use onsite storage of backups to ensure information is able to be recovered quickly in the event of disruptions or damage that does not render the normal production site unusable. [CP-9].

3. Document backup media storage locations and retention dates in the information SSPs and ISCPs.

4. Document procedures for testing backup media/information. Test backup information to verify media reliability and information integrity. [CP-9(1)]

5. Clean, store, and rotate backup media to guard against media failure according to vendor or software recommendations.

6. Ensure backup and recovery equipment maintenance meets levels no less than the minimum manufacturer recommendations.

7. Sanitize or destroy backup media before it is transferred, sold, or otherwise disposed of or allowed to be used for other purposes. Use sanitization and disposal methods appropriate for the information's FIPS 199 security categorization, following guidelines found in NIST SP 800-88 Rev. 1.

8. Properly label all backup media.

9. Physically secure backup and recovery systems and media, restricting access to only those that require it for their official duties. Protect the confidentiality and integrity of the backup information at the storage location. [CP-9]

10. Maintain a list of personnel or positions authorized to access backup media in information SSPs and ISCPs.

11. Perform periodic security checks to verify media are being properly handled and stored according to the requirements of the security plan.

12. Use an alternate storage site to ensure ability to recover from disasters or disruptions that render the primary production site unusable or that damage or destroy onsite backup media:

    a. Store monthly or full system backups at an alternate storage site in accordance with applicable record management and retention policy unless otherwise required by the information system's ISCP. [CP-9(3)]

    b. Rotate backup files to an alternate storage site as required by the information system's security plan.

13. Control and document all removal, use, and return of backup media, including access to backup media storage areas or facilities to include person, reason, specific media, where the media will be taken, and date/time of removal and return.

6683.48 - System Recovery and Reconstitution

1. Develop recovery and reconstitution strategies, activities, and detailed procedures to recover and reconstitute processing capabilities to a known state after a

disruption, compromise, or failure, repair damage to the original system, restore operational capabilities at the primary or alternate facility, and recover from information system compromise. [CP-10]

2. Complete a location specific Business Impact Analysis (BIA) to determine the appropriate recovery priority and allowable outage times for information systems, applications, and system components.

3. Assign contingency roles and responsibilities to personnel and teams responsible for information systems.

4. Ensure the information system implements transaction recovery for systems that are transaction-based. [CP-10(2)]

5. Employ compensating controls for circumstances that would prevent recovery to a known state.

6683.48a - Disaster Recovery and Reconstitution

1. Develop an ISCP for each major information system when an emergency or other event makes the system inoperable or inaccessible. [CP-2]

2. Develop ISCPs using the appropriate Forest Service version of the USDA ISCP Template.

3. Develop ISCPs in conjunction with BRPs so that the transition from system recovery to business resumption during and after an emergency or disruption is orderly and efficient.

4. Coordinate ISCPs with Continuity of Operations Plans (COOPs) so there are no conflicts of responsibility or authority.

5. Review and test, at least as a tabletop exercise, each ISCP as required to ensure that it can be executed and will fulfill its intended purpose, of quickly returning a disrupted or damaged information system to operability. Perform functional tests of each mission essential or mission critical application and general support systems (GSSs), unless not cost effective, in which case the system owner shall request and obtain a waiver from the ACISO to conduct partial functional tests or other less costly tests that can accurately gauge effectiveness of the recovery plan. Correct any deficiencies in the plan discovered during testing. [CP-4]

6683.5 - Hardware and System Software Maintenance

6683.51 - Controlled and Nonlocal Maintenance and Maintenance Tools

Schedule, perform, document, and review preventive and regular maintenance activities: [MA-2, MA-3]

1. Maintain a maintenance log for the life of each IT system component.

2. Control all maintenance activities utilizing the IT system's documented procedures for unscheduled and scheduled maintenance and ensuring designated officials explicitly approve the removal of any information system component from a Forest Service facility.

3. Test maintenance activities and media in advance of implementation to ensure the action may not harm the IT environment. [MA-3(2)]

4. Inform all users of scheduled, unscheduled, and emergency maintenance on the IT system that may impact their use of the system, and notification should be provided as far in advance as feasible.

5. Obtain required approvals for all hardware and software introduced to the system specifically for diagnostic/repair actions (maintenance tools) prior to use and monitor use of the tools.

6. Test and verify maintenance tools to ensure they cannot or will not cause any damage to Forest Service systems. [MA-3(1)]

7. Complete non-local maintenance activities in accordance with available, standard CIO-approved procedures and without significantly affecting information system security, availability, or performance. Ensure that all non-local maintenance and diagnostic activities are authorized, logged, and audited. The Forest Service will employ strong identification and authentication techniques for non-local maintenance and diagnostic sessions. Document the installation and the use of non-local maintenance and diagnostic connections in the information system SSP. [MA-4]

8. Terminate all sessions and remote connections when remote maintenance is completed.

9. Sanitize equipment, as appropriate, to remove all information from associated media prior to removal from Forest Service facilities for off-site repair or maintenance. [MA-3(3)]

6683.52 - Maintenance Personnel

1. Perform timely and complete maintenance of Forest Service systems to be conducted only by authorized personnel. [MA-5]

2. Establish a process for maintenance personnel authorization. Maintain a list of all authorized personnel who perform maintenance on information systems. [MA-5]

3. Escort maintenance personnel who do not have the required level of access to the information system(s) being serviced. [MA-5]

4. Authenticate non-Forest Service maintenance personnel through the use of pre-planned appointments and identification checks. [MA-5]

5. Require that non-Forest Service maintenance personnel have continuous supervision by a Forest Service authorized individual who has the appropriate level of access to the system(s) undergoing maintenance and technical competence deemed necessary. [MA-5]

6. Detail maintenance personnel screening and access requirements in the statement of work or contract covering the information system's maintenance.

6683.53 - Timely Maintenance

1. Identify key information system components. Document in the information system SSP for which components it will obtain maintenance support and/or spare parts and the time frame required. [MA-6]

2. Review service provider contracts or service level agreements for information system maintenance to ensure that they provide: [MA-6]

    a. Regular, scheduled preventative maintenance and key component replacement parts.

    b. Emergency maintenance support and key component replacement parts as defined in the information system SSP.

3. Provide regularly scheduled maintenance in accordance with the information system component manufacturer's recommendations (at a minimum) and as specified in the SSP. [MA-6]

4. Maintain an adequate inventory or contract provisions for replacement that ensure key component spare parts are available within a specified period of time. [MA-6]

6683.6 - Security Awareness and Training

6683.61 - Security and Privacy Training and Awareness

1. Ensure that all information system users (including Managers, Senior Executives, Contractors, and temporary employees) receive basic security and privacy awareness training and accept the rules of behavior before they are authorized to access the system. [AT-2]

2. Provide basic security and privacy awareness training for information system users immediately when beginning employment and yearly thereafter and whenever required by information system changes. [AT-2a]

3. Determine the appropriate content of security and privacy awareness training based on the specific requirements of the Forest Service and the information systems to which personnel have authorized access, recognizing and reporting potential indicators of insider threats and both potential and actual instances of social engineering and social mining. Update as directed by USDA. [AT-2c, 2(2), 2(3)]

4. Employ security and privacy awareness techniques such as displaying posters, logon screen messages and electronic messaging boards. [AT-2b, 3c]

6683.62 - Information Security Training

1. Develop, implement and maintain a Forest Service-wide program of role-based security and privacy training for those with additional information system security responsibilities. [AT-3]

2. Identify personnel who have significant information system security and privacy roles and responsibilities during the system development life cycle and document those roles and responsibilities. [AT-3]

3. Provide appropriate role-based information system security and privacy training: [AT-3]

    a. Before authorizing access to the system or performing assigned duties;

    b. For all new or newly assigned system users or Managers, System Administrators, and other personnel with access to system level software and having additional information system security or privacy responsibilities;

    c. Whenever there is a significant change in direction, a major system modification, a significant software change, or a change of duties; and

    d. As required thereafter.

e. For roles that process PII including in privacy notices, systems of record notices, computer matching agreements and notices, and privacy impact statements, contracts, memoranda of understanding, information sharing agreements and other documentation. [AT-3(5) PRIV]

4. Ensure that those involved in the design, development, operation, management, or maintenance of an information system or application are aware of their security and privacy responsibilities based on their level of access and are trained to fulfill those responsibilities. [AT-3]

5. Design security and privacy training programs to take advantage of current technology and lessons learned from internal or external security breaches that provides ease of use, scalability, accountability, and reliable support, to the extent possible. [AT-3c]

6. Ensure that the role-based IT security and privacy training program is consistent with NIST and Federal guidance, addressing management, operational, and technical roles. [AT-3]

6683.63 - Training Records

1. Document and monitor individual information system security and privacy training activities including basic security and privacy awareness training and specific (role-based) information system security and privacy training for personnel with significant IT security or privacy roles and responsibilities. [AT-4]

2. Retain security and privacy training records in accordance with Federal record retention requirements. [AT-4]

3. Ensure Forest Service personnel take required training or work with system managers to disable access until training is completed.

4. Ensure that Forest Service personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements.

6683.7 - System and Services Acquisition

6683.71 - Allocation of Resources

1. Include a determination of information security and privacy requirements for the information system in mission/business process planning. [SA-2]

2. Determine, document, and allocate the resources required to protect the information system as part of the Forest Service's capital planning and investment control process. [SA-2]

3. Establish a discrete line item for information security in organizational programming and budgeting documentation. [SA-2]

6683.72 - Acquisition Process

The Forest Service includes the following requirements, criteria, and/or specifications, as appropriate, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards and the Forest Service's mission/business needs: [SA-4]

1. Security and privacy functional, strength, and assurance requirements and specifications.

2. Security- and privacy-related documentation requirements, including controls needed and requirements on protecting security-related documentation.

3. Acceptance criteria.

4. Identification of parties responsible for information security, privacy, and supply chain risk management.

5. Developmental and evaluation-related assurance requirements.

6. The employment/use of only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems. [SA-4(10)]

7. The requirement that developers provide information describing the functional properties of the security and privacy controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls and these requirements are made available to authorized personnel. [SA-4(1)]

8. The requirement that developers provide design and implementation information for the security and privacy controls to be employed within the information system, information system components, or information system services at the appropriate level of detail. [SA-4(2)]

9. The requirement that developers provide information describing the information system development environment and environment in which the system is intended to operate.

10. The requirement that the developer of the information system, system component, or information system service identify early in the system development life cycle the functions, ports, protocols, and services intended for organizational use. [SA-4(9)]

11. The requirement that each information system component acquired is explicitly assigned to an information system, and that the owner of the system acknowledges this assignment.

6683.8 - Security and Privacy Engineering Principles

1. The Forest Service will apply information system security and privacy engineering principles in the specification, design, development, implementation, and modification of the information system and system components. [SA-8]

2. Implement the privacy "principle of minimization" when processing PII. [SA-8(33) PRIV]

6683.81 - External System Services

1. Apply system security engineering principles in the specification, design, development, implementation, and modification of the information system and system components. [SA-8]

2. Require providers of external system services to comply with Forest Service information security and privacy requirements and employ appropriate security controls in accordance with the applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. [SA-9]

3. Define and document Government oversight and user roles and responsibilities with regard to external information system services. [SA-9]

4. Monitor security control compliance by external service providers. [SA-9]

5. Require external system services to identify the functions, ports, protocols, and other services intended for organizational use. [SA-9(2)]

6683.81a - Developer Configuration Management

1. The Forest Service requires that developers/integrators of information systems, system component, or system service will: [SA-10]

    a. Perform configuration management during information system, component or service design, development, implementation, and operation,

b. Manage and control changes to the information system, component, or service,

c. Implement only organization-approved changes,

d. Document approved changes to the information system, component, or service,

e. Track security flaws and flaw resolution within the system, component, or service, [SA-10]

f. Develop and implement a plan for ongoing security and privacy control assessments, [SA-11]

g. Perform system, component or service testing/evaluation and produce evidence of testing and evaluation results, [SA-11]

h. Implement a verifiable flaw remediation process, [SA-11]

i. Correct flaws identified during testing and evaluation, [SA-11]

j. Follow a plan to explicitly address security and privacy requirements, [SA-15]

k. Identify the standards and tools used in the development process, [SA-15]

l. Document the specific tools and options and tool configurations used in the development process, [SA-15]

m. Document, manage, and ensure the integrity of changes to the process and/or tools used in development, [SA-15]

n. Perform a criticality analysis when the architecture or design is modified or upgraded. [SA-15(3)]

2. Review the development process, standards, tools, tool options, and tool configurations to determine if the process, standards, tools, tool options, and tool configurations selected can satisfy the security and privacy control requirements. [SA-15]

6683.81b - System and Information Integrity

1. Develop and implement controls and procedures for flaw remediation, malicious code, spam, and spyware protection; intrusion detection; and security.

2. Implement Intrusion Detection Systems, and malicious code detection and elimination software.

3. Implement reconciliation routines on systems that support this capability (that is, checksums, hash totals, record counts).

4. Periodically confirm the integrity of system controls using password crackers and checkers.

5. Confirm the integrity of system boundary protections from external attack(s) using periodic system penetration testing.

6. Use message authentication in systems that support this capability to ensure that the sender of a message is known and that the message has not been altered during transmission.

7. Use encryption methods specified in DM 3530-005 Encryption Security Standards to protect information transferred over any private information carrier to and from USDA network access points.

8. Encrypt Sensitive but Unclassified (SBU) information before it leaves the Forest Service network when it is traversing external connection.

9. If an information system breach is suspected, use integrity verification programs to look for evidence of information tampering, errors, and omissions.

6683.82 - Flaw Remediation

1. Identify, report, and correct software flaws and vulnerabilities in accordance with Forest Service configuration management (CM) and emergency change policy. [SI-2]

2. Test software and firmware updates, patches, fixes, or similar corrective updates for effectiveness and potential side effects before applying them. [SI-2]

3. Install security-relevant software and firmware updates within USDA-provided timeframes of the software or firmware release. [SI-2]

4. Incorporate flaw remediation into the system configuration management process. [SI-2]

5. Determine if system components have applicable security relevant software and firmware updates installed using automated mechanisms. [SI-2(2)]

6. Use approved Forest Service automated tools to check the status of flaw remediation on an ongoing basis.

6683.83 - Malicious Code Protection and Spam Control

1. Employ and update automatically on a regular basis a protection mechanism on Forest Service information systems—primarily at entry and exit points, workstations, servers, and mobile computing devices on the network—to detect and eradicate malicious code that is: [SI-3]

    a. Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means. [SI-3]

    b. Inserted through the exploitation of information system vulnerabilities. [SI-3]

2. Ensure that, when detected, malicious code will be quarantined and blocked, and a notification will be sent to the System Administrator.

3. Configure malicious code protection mechanisms to perform periodic scans of the information system and real-time scans of files from external sources and to send an alert to a System Administrator in response to malicious code detection. [SI-3]

4. Employ spam protection mechanisms at critical information system entry and exit points and workstations, servers, and mobile computing devices on the network to detect and act on unsolicited messages. [SI-8]

5. Automatically update spam protection mechanisms when new releases are available. [SI-8, 8(2)]

6. Ensure action is taken on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means.

7. Provide for centrally managed malicious code and spam protection mechanisms.

8. System Administrators will determine if the malicious code is a false positive and the resulting potential impact on the availability of the system. [SI-3]

6683.84 - System Monitoring

1. Identify types of activities or conditions considered unusual or unauthorized. [SI-4(4)]

2. Monitor the system and all inbound and outbound communications traffic to detect attacks, indicators of potential attacks, unauthorized activities/conditions and local, network or remote connections. [SI-4(4)]

3. Respond, as appropriate, to any real or perceived threat disclosed by monitoring activities. [SI-4]

4. Deploy monitoring devices throughout the system to continually monitor connections and at ad-hoc locations when indications of compromise or potential compromise occur. [SI-4]

5. Analyze detected events and anomalies and protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion. [SI-4, 4(2)]

6. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to Forest Service operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources. [SI-4]

7. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable Federal laws, Executive Orders, directives, policies, or regulations. [SI-4]

8. Provide information system monitoring information to appropriate Forest Service personnel. [SI-4]

6683.85 - Security Alerts, Advisories and Directives

1. Subscribe to reliable alert and advisory sources.

2. Review security alerts and advisories as they are received. [SI-5]

3. Implement applicable alerts and advisories in accordance with established time frames, and document actions taken. As directed, notify issuing organization of the degree of compliance. [SI-5]

4. Generate internal security alerts, advisories, and directives as deemed necessary. [SI-5]

5. Disseminate security alerts, compromises, advisories, and directives to the ACIO for NRE, the ACISO, ISSOs, System Administrators, and other agency-designated individuals with security roles or responsibilities. [SI-4(5)]

6683.86 - Software, Firmware, and Information Integrity

1. Employ integrity verification tools to detect changes to unauthorized software, firmware, and information. [SI-7]

2. Ensure that the information system performs an integrity check of software and information by performing periodic integrity scans of the information system. [SI-7(1)]

3. Incorporate the detection of unauthorized changes to the information system into the organizational incident response capability. [SI-7(7)]

6683.86a - Information Input Validation

The Forest Service will design the information system to check information for validity as close to the point of information input as possible, in accordance with organizational policy and operational requirements including the following: [SI-10]

1. Design the information system to check information for validity as close to the point of information input as possible. [SI-10]

2. Design the system to prescreen inputs to ensure the content is not unintentionally interpreted as commands. [SI-10]

3. Design the system to employ rules for checking the valid syntax of information system to ensure that inputs match specified definitions for format and content. [SI-10]

4. Configure server applications to prohibit invalid information from clients in order to mitigate application vulnerabilities such as buffer overflow, cross-site scripting, null byte attacks, SQL injection attacks, and HTTP header manipulation. [SI-10]

5. Ensure invalid inputs or error statements do not give the user sensitive information, storage locations, database names, or information about the application or IT system's architecture. [SI-10]

6683.86b - Error Handling

1. Design systems to generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. [SI-11]

2. Design systems to reveal error messages only to authorized personnel. [SI-11]

3. Develop error messages and/or associated administrative messages and error logs so that they do not contain sensitive information (for example, account numbers, social security numbers, and credit card numbers).

6683.86c - Information Management and Retention

1. Handle and retain information within the information system and information output from the information system in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. [SI-12]

2. Label output from the information system when appropriate.

3. Retain output from the information in accordance with Federal record retention policies.

6683.87 - Memory Protection

The information system must implement appropriate security safeguards to protect its memory from unauthorized code execution. [SI-16]

6683.88 - Risk Assessment

6683.88a - Security Categorization

1. Categorize information and the information system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and applicable guidance. [RA-2]

2. Document the critical components/functions and security categorization results in the security plan for the information system. [RA-2]

3. Ensure the security categorization is reviewed and approved by the Authorizing Official or his/her representative. [RA-2]

6683.88b - Vulnerability Monitoring and Scanning

1. Scan for vulnerabilities in the information system and hosted applications as required and when new vulnerabilities that potentially may affect the system and application are identified and reported. [RA-5]

2. Using the approved USDA vulnerability scanning tools to promote interoperability among tools and automate parts of the vulnerability management process by using standards for: [RA-5]

    a. Enumerating platforms, software flaws, and improper configurations;

    b. Formatting checklists and test procedures; and

    c. Measuring vulnerability impact.

3. Analyze vulnerability scan reports and results from security control assessments. [RA-5]

4. Make recommendations on remediation of legitimate vulnerabilities within the USDA-established time limits in accordance with the Forest Service assessment of risk. [RA-5]

5. Share information obtained from the vulnerability scanning process across the Forest Service and with USDA to help eliminate similar vulnerabilities in other information systems. [RA-5]

6. Employ vulnerability scanning tools that include the capability to readily update the list of vulnerabilities scanned. [RA-5]

7. Update the list of information system vulnerabilities scanned prior to a new scan and when new vulnerabilities are identified and reported. [RA-5(2)]

8. Configure information systems to implement privileged access authorization to appropriate information systems components for specific vulnerability scanning activities. [RA-5(5)]

9. Establish a public reporting channel for reporting vulnerabilities in systems and system components. [RA-5(11)]

6683.9 - Additional Security Operational Controls for High Value Asset Systems

Note: These policies only apply to information systems designated by USDA as a High Value Asset (HVA) System.

6683.9a - Security Literacy Training and Awareness

Provide practical exercises in security awareness training that simulate events and incidents. [AT-2(1)]

6683.9b - Configuration Change Control

Prevent or restrict changes to system configurations that affect critical system security and privacy functionality. [CM-3(7)]

6683.9c - Impact Analysis

Analyze changes to the system, looking for security and privacy flaws, in a separate test environment before implementing in an operational environment, [CM-4(1)]

6683.9d - Configuration Settings

Take appropriate actions, including alerting designated personnel, to unauthorized configuration changes. [CM-6(2)]

6683.9e - Telecommunication Services

Test alternative telecommunications services as specified in the system security plan. [CP-8(5)]

6683.9f - System Recovery and Reconstitution

Provide the capability to restore system components from configuration-controlled and integrity-protected information, representing a known, operational state for the components. [CP-10(4)]

6683.9g - Media Sanitation

Provide remote capability to purge or wipe information from systems or system components. [MP-6(8)]

6683.9h - Physical Access Control

Enforce physical system access authorizations, in addition to physical access controls. [PE-3(1)]

6683.9i - System Monitoring

1. Connect and configure individual intrusion detection tools into a system-wide intrusion detection system. [SI-4(1)]

2. Ensure all encrypted communications traffic is visible to system monitoring tools. [SI-4(10)]

3. Analyze outbound communication traffic at all external system interfaces and selected interior points to discover anomalies. [SI-4(11)]

4. Analyze communication patterns and event patterns, develop profiles representing common traffic and event patterns, and use the traffic and event profiles to tune system monitoring devices. [SI-4(13)]

5. Correlate information from monitoring tools employed throughout the system. [SI-4(16)]

6. Analyze outbound communications traffic at external interfaces to the system and at interior points to detect covert exfiltration of information. [SI-4(18)]

7. Implement additional monitoring of privileged users. [SI-4(20)]

8. Detect unauthorized and unapproved network services and alert authorized personnel when detected. [SI-4(22)]

9. Implement host-based monitoring mechanisms on system components. [SI-4(23)]

6684 - Security Technical Controls

6684.01 - Authority [Reserved]

6684.02 - Objective

The objectives of technical security controls are to protect the confidentiality, integrity, and availability of the information, information systems, and information technology (IT) that support the Forest Service mission by:

1. Implementing safeguards which are executed by the operating system in the hardware, software, or firmware components of information systems.

2. Ensuring that responsible employees are clearly and explicitly informed about technical requirements and procedures within their realm of influence that secure IT resources.

3. Providing an effective Forest Service response to technical security threats and breaches.

4. Promoting continuous monitoring capabilities through the development and maintenance of efficient processes and procedures.

6684.03 - Policy [Reserved]

6684.04 - Responsibility

6684.04a - Assistant Chief Information Officer for Natural Resources and Environment

The ACIO for NRE is responsible for:

1. Ensuring that Forest Service IT systems allow all Forest Service IT personnel involved in implementing or maintaining password and other access control requirements to have the appropriate background investigation or clearance, and that appropriate separation of duties is maintained.

2. Ensuring that formal procedures and practices for controlling access to Forest Service information systems are in place and being followed.

6684.04b - Assistant Chief Information Security Officer for NRE

The ACISO for NRE is responsible for:

Advising CIO leadership team and system personnel of security implications and ramifications of new of revised configuration management proposals.

6684.04c - Information System Security Manager

Information System Security Managers are responsible for:

Participating in the Forest Service Configuration Control Board as a member and advising on technology and emerging threats.

6684.04d - System Owners

System owners are responsible for:

1. Determining the security categories of and sensitivity of the information processed or contained in the systems, programs or files for which they are responsible, as described in NIST FIPS Publication 199, “Standards for Security Categorization of Federal Information and Information Systems.”

2. Determining which additional auditing information will be collected, based on the security categories of the systems for which they are responsible.

3. Ensuring information systems audit and produce records for the events and privileged functions identified in the system’s SSP and provide the capability for audit reduction and audit report generation.

4. Ensuring that the Forest Service information system generates time stamps for use in audit record generation.

5. Utilizing a common time source to ensure the enterprise IT system clocks are synchronized.

6. Ensuring that audit trails and audit logs are protected from unauthorized modification, access, or destruction while online and during offline storage.

7. Ensuring that privileges to disable auditing are restricted to authorized personnel.

8. Ensuring that user accounts conform to USDA identity management standards, are created, modified, or deleted only when properly requested by a Supervisor or other authorized person, and are disabled upon discovery of reliable evidence of a significant security or privacy risk.

9. Ensuring audit logs are retained and preserved for integrity, which include system, application, and database-level audit logs, as required to provide support after the fact investigations of IT security incidents or a potential incident is known, and to meet regulatory and organizational information retention requirements.

10. Documenting a mechanism, either automated or manual, for managing all cryptographic keys in use by the system.

11. Approving user roles and the associated privileges/permissions for the systems they are accountable for.

12. Overseeing accurate and routine completion of the system account review process on a regular basis.

13. Reporting alleged or suspected criminal activity to LEI immediately.

14. Identifying, defining, and ensuring implementation of appropriate checklists/settings and document secure baseline configurations for all responsible systems.

15. Ensuring that systems comply with the approved hardware and software lists.

16. Ensuring that change controls are in place and functioning properly.

17. Ensuring the development and maintenance of an inventory of their information systems.

18. Approving procedures, mechanisms, or protocols that are used for host or device authentication.

19. Ensuring that IT devices are configured with synchronized internal information system clocks.

20. Ensuring that a common time source is available for IT systems to synchronize.

21. Ensuring that separation of duties exists between information system personnel who administer the access control function and those who administer the audit trail.

22. Ensuring that sessions to IT systems are configured to automatically lock or terminate after a specified period of inactivity.

23. Managing system identifiers and authenticators used to access information systems.

24. Providing for individuals' ability to review their own PII held within agency records, regardless of format.

25. Documenting, in the system security plan, all user actions allowed on information systems without identification or authentication.

26. Employing mechanisms to assist authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions.

27. Configure all Forest Service information systems to accept and electronically verify Personal Identity Verification-compliant credentials from other federal agencies for authorized personnel where possible.

28. Accept only external authenticators that are NIST-compliant. In the system security plan, document and maintain a list of accepted external authenticators.

29. Establishing usage restrictions and implementation guidance for wireless access and authorizing wireless access to the information system prior to granting access to the information system.

30. Disable wireless networking capabilities embedded within system components, when not intended for use.

31. Establishing and documenting usage restrictions, configuration. connection requirements, and implementation guidance for each type of remote access and managing the remote access to authorized users.

32. Establishing configuration requirements, connection requirements, and implementation guidance for mobile devices, including when mobile devices are outside of controlled areas and managing the mobile devices.

33. Monitoring and controlling communications at the external boundary of the Forest Service network and at key internal boundaries within the Forest Service network. Limiting the number of external connections.

34. For systems that process PII, monitoring permitted processing rules for data elements of PII, documenting each exception, and reviewing and removing exceptions that are no longer supported.

6684.04e - Information System Security Officers

Information System Security Officers are responsible for:

1. Verifying that information system access and accounts are properly authorized and current. Ensuring review of access according to the system security plan requirements.

2. Documenting and monitoring security controls of systems assigned to ISSO.

3. Notifying the System Owner of any security control implementation discrepancies.

6684.04f - Supervisors

Supervisors requesting access to information systems on behalf of their employees, contractors, and cooperators, shall follow the procedures of the system security plan and/or operations guide and are responsible for:

1. Requesting system access using the process referenced in the system security plan or operations guide for the individual information system and verifying that the level of access requested is the minimum necessary for the individual to accomplish assigned tasks.

2. Requesting transfers or termination of system access when an employee transfers or leaves the Forest Service.

3. Requesting immediate termination of system access in cases of termination for cause.

4. Requesting modification of system access when a change of duties to a position necessitates a change in the employee's access rights.

5. Holding employees accountable for removal of software identified as being prohibited, unauthorized, or malicious software (malware) from Forest Service computers in their possession or under their control, and for which direction has been issued by the CIO Cybersecurity Internal Controls Branch Chief requiring its removal.

6. Assisting in the resolution of disputes between employees and the CIO Cybersecurity Internal Controls Branch Chief over whether software on end user computers identified as being unauthorized serves a legitimate business purpose.

7. Reporting, immediately, suspected, or alleged IT-related security violations, misconduct, or criminal activity to the information System Security Officer or the USDA, CIRRB.

6684.04g - End Users

End users are responsible for:

1. Reporting any known or suspected password or other authenticator compromise or loss to the USDA, CIRRB, their Supervisor or Contracting Officer.

2. Changing any password or other authenticator or immediately upon suspicion or detection of its compromise.

3. Maintaining privileged end users and their use of a separate nonprivileged system account and password for nonprivileged access to systems or applications.

4. Notifying their Supervisor of any instance in which they do not have the necessary access rights to an application or system to perform the official duties of their position.

5. Acknowledging receipt of direction from USDA, CIRRB to remove software identified as being unauthorized, prohibited, or malware. After such acknowledgment immediately remove or request assistance through the Customer Help Desk to remove such software from Forest Service-owned desktop and laptop computers in their possession or control.

6. Reporting suspected or alleged IT related security violations, misconduct, or criminal activity to their Supervisor or the USDA, CIRRB, immediately.

6684.04h - System Administrators

System Administrators are responsible for:

1. Maintaining and using a separate user account and authenticator for system administration or other privileged system or application access.

2. Ensuring that server system logs are configured, maintained, and available for review by authorized individuals.

3. Processing requests to create, modify, or delete accounts on Forest Service information systems when requested by a Supervisor or other authorized person, using the process required by the system security plan or operations guide.

4. Ensuring that routine system monitoring processes are operational.

5. Reporting, immediately, evidence of suspected or alleged employee security violations detected during system operation or monitoring to the USDA, CIRRB.

6. Ensuring media containing Forest Service information has been rendered unreadable as part of disposal process.

7. Assisting with the system account review process.

8. Assisting with implementation of security controls.

9. Alert system owners and ISSOs to unauthorized access, modification, or deletion of system audit information.

6684.04i - Generic System Access Account Managers

Generic system access Account Managers are responsible for:

1. Requesting the generic access account from their Supervisor.
2. Assigning one (and only one) user to the specific account at a time.
3. Changing account passwords prior to assignment and after assignment.
4. Limiting system access when the account is not assigned to an individual.
5. Documenting who has access to the account and when.
6. Ensuring that users conform to applicable policies and procedures.
7. Monitoring the actions performed by those persons using these accounts.

6684.04j - Account Sponsors

Account sponsors are Forest Service employees requesting access to Forest Service information systems on behalf of their volunteers, cooperators, and contractors. Account sponsors are responsible for:

1. All supervisory duties for volunteers, contractors, and cooperators.
2. Requesting system access using the process referenced in the system security plan or operations guide for the individual information system and verifying that the level of access requested is the minimum necessary for the individual to accomplish assigned tasks.
3. Requesting transfer or termination of system access when a volunteer, cooperator, or contractor transfers or leaves the Forest Service.
4. Requesting immediate termination of system access in cases of termination for cause.
5. Requesting modification of system access when a change of duties to a position necessitates a change in the volunteer, cooperator, or contractor’s access needs.
6. Holding volunteers, cooperators, and contractors under their responsibility accountable for removal of software identified as being prohibited, unauthorized, or malicious software (malware) from Forest Service computers in their possession or

under their control, and for which direction has been issued by the CIO Cybersecurity Internal Controls Branch Chief requiring its removal.

7. Assisting in the resolution of disputes between volunteers, cooperators, and/or contractors under their responsibility, and the CIO Cybersecurity Internal Controls Branch Chief, whether software on end user computers identified as being unauthorized serves a legitimate business purpose.

8. Reporting suspected or alleged IT-related security violations, misconduct, or criminal activity to the Information System Security Officer or the USDA, CIRRB, immediately.

9. Ensuring that volunteers, cooperators, and contractors under their responsibility are notified of all Forest Service information security responsibilities and formally accept those responsibilities before gaining access to any Forest Service information system.

10. Ensuring that volunteers, cooperators, and contractors under their responsibility undergo required personnel screening commensurate with their assigned responsibilities.

11. Entering and maintaining relationship information on behalf of volunteers, cooperators, and contractors under their responsibility into the USDA Non-Employee Information System in accordance with established USDA and Forest Service procedures.

6684.1 - Identification and Authentication

6684.11 - Identifier and Authenticator Management

1. Allow logical access to Forest Service information systems only with user identification and authentication, except for systems intended for public access, such as web-based applications delivering general information approved for distribution to the public. [IA-2]

    a. For each user, issue a unique user account which verifies the user's identity.

    b. Only appropriate Forest Service officials may issue user accounts including but not limited to PIV authentication, and other types of hardware type access devices, after the Supervisor has established the identity of the user.

    c. Individual identification is required at the registration authority to receive a PIV credential. Identification information will be verified by appropriate authorities.
    [IA-12(2), (3)]

d. Confirmation emails will be sent to the individual's personal email to verify user's address or record. [IA-12(5)]

e. Deactivate user accounts after the period of inactivity.

f. Manage system identifiers by: [IA-4]

(1) Receiving authorization from Supervisor to assign an individual, group, role, service, or device identifier.

(2) Selecting an identifier for an individual, group, role, service, or device.

(3) Assigning the identifier to the individual, group, role, service, or device.

(4) Preventing reuse of identifiers.

(5) Uniquely identifying each individual as employee, contractor, foreign national, or non-Forest Service user. [IA-4(4)]

g. Manage system authenticators used to access information systems by: [IA-5]

(1) Verifying the identity of the individual, group, role, service, or device receiving the authenticator.

(2) Establishing initial authenticator content.

(3) Ensuring the authenticator has sufficient mechanism strength for their intended use.

(4) Establishing and implementing administrative procedures for initial authenticator distribution; for lost or compromised or damaged authenticators and revoking authenticators.

(5) Changing default authenticators before first use.

(6) Changing or refreshing authenticators.

(7) Protecting authenticator content from unauthorized disclosure and modification.

(8) Requiring individuals to protect authenticators.

(9) Changing authenticator for group accounts when group membership changes.

(10) Obscure the feedback of authentication information during the authentication process. [IA-6]

h. Employ secure two-factor authentication mechanisms for network access to non-privileged accounts and local access to privileged accounts. Non-local access to privileged accounts employs replay-resistant authentication mechanisms. [IA-2(1), IA-2(2), IA-2(8)]

i. Default authenticators must be changed upon information system installation.

2. Take reasonable measures to safeguard authenticators from unauthorized disclosure and modification, including, but not limited to maintaining possession of authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators in a timely manner. [IA-5(6)]

3. Employ mechanisms to ensure that the identification and authentication of users is enforced before system access is granted.

4. Require users to re-authenticate when credentials change, roles change, or security categories of the system change. [IA-11]

6684.12 - Password Content Requirements

6684.2 - Access Controls

1. Implement local certificate revocation data to support path discovery and validation in case of inability to access revocation information via the network.

2. Develop procedures for authenticator distribution, dealing with lost, compromised, or damaged authenticators, for revoking authenticators, changing default authenticators upon information system installation. [IA-5]

3. Ensure Forest Service information systems conform to USDA-approved identity management profiles. [IA-8(4)]

4. Require use of separate accounts for privileged and non-privileged access to IT systems and devices.

5. Require multi-factor authentication capability for both privileged and non-privileged account authentication. [IA-2(1), 2(2)]

6. Do not allow privileged accounts direct access to the internet or email.

7. Configure all password-protected information systems to display an approved system use notification warning banner before granting access that states the following: [AC-8]

    a. Users are accessing a U.S. Government information system.

    b. System usage may be monitored, recorded, and subject to audit; and

    c. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

    d. Use of the system indicates consent to monitoring and recording.

8. Retain the notification message or banner on the screen until users take explicit actions to log on to or further access the information system. [AC-8]

9. Configure all password-protected IT resources to automatically lock user accounts after a fixed number of attempts during a specified time period in the SSP until released by an Administrator, and/or delay the next logon prompt. Exceptions or deviations from this lockout process and lockout time duration must be documented in the SSP along with the accompanying compensating control. [AC-7]

10. When no interaction occurs between a user and an information system for a period in excess of the inactivity time limit specified in the system's security plan, ensure that the information system either: [AC-11, 12]

    a. Locks the session to ensure that users must reenter their passwords to resume the session.

    b. Terminates the session, requiring users to log back into the application.

11. When no interaction occurs between a user and the user's computer or workstation (desktop or laptop) for a period of time, ensure that the computer's operating system invokes a screen saver that requires the user to re-enter their password to regain access to the computer. [AC-11(1)]

12. Allow remote access to Forest Service information systems only through Forest Service controlled Virtual Private Network (VPN) and portal facilities located in the Forest Service DMZ, or equivalent trusted authentication devices or procedures.

13. For publicly accessible systems: [AC-8]

a. Display the system use information when appropriate before granting further access.

b. Display references to monitoring, recording, or auditing that are consistent with privacy accommodations for those systems that generally prohibit such activities.

c. Include in the notice given to public users of the information system a description of the authorized uses of the system.

14. Configure all Forest Service information systems such that access to privileged functions as listed in the system security plan (deployed in hardware, software, and firmware) and to security relevant information is restricted to explicitly authorized personnel (for example, security administrators, system administrators, and other privileged users).

15. Provide for individuals' ability to review their own PII held within agency records, regardless of format. [AC-3(14) PRIV]

6684.21 - Account Management

1. Manage all information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Review all information system accounts as required. [AC-2f]

2. Employ automated mechanisms to support the management of information system accounts. [AC-2(1)]

3. Assign Account Managers to all information system accounts. [AC-2b]

4. Configure all Forest Service information system emergency accounts such that they are automatically disabled as soon as not needed. [AC-2l, AC-2(2)]

5. Configure all Forest Service information systems such that they automatically disable accounts after periods of inactivity as stated in the SSP and in accordance with USDA policy. Remove inactive accounts after an additional period of inactivity except as specified. [AC-2l, AC-2(2), (3), (5)]

6. Disable individuals' accounts upon discovery of reliable evidence of a significant security or privacy risk. [AC-2(13)]

7. Require appropriate approval of requests to establish accounts. [AC-2e]

8. Identify-proof the users identity information to establish credentials. [IA-12]

9. Ensure automated mechanisms are employed to audit account creation, modification, disabling, and termination actions and notify, as required, appropriate individuals.
   [AC-2g, h, AC-2(4)]

10. Ensure that the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users). [IA-8]

11. Ensure that all account creation, modification, disabling, and termination actions are audited, including audit of the administrative accounts that conduct the actions.

12. Document access management processes, access methods, and approval/denial decisions in a manner that creates evidence of compliance that is available for approved audits, data calls, and continuous monitoring reviews. [AC-2j]

6684.22 - Access Enforcement

1. Configure all Forest Service information systems such that they enforce assigned authorizations for controlling logical access to the system. If encryption of stored information is used as an access enforcement mechanism, use only cryptography that is compliant with applicable Federal standards. [AC-2i, AC-3]

2. The following conditions must be met prior to obtaining access to systems operated by or on behalf of the Forest Service:

   a. Users shall have a current, successful background investigation.

   b. Users shall successfully complete training in information security awareness, personally identifiable information (PII), and rules of behavior.

   c. Enforce the use of human review of user information when the system is not capable of making an information flow control decision. [AC-4(9)]

3. Implement a controlled, audited, and manual override of automated mechanisms, when appropriate, to handle an emergency or other serious event.

4. Configure the information system to enforce approved authorizations for controlling the flow of information within the system and between interconnected systems. [AC-4]

5. Document, in the system security plan, all user actions allowed on information systems without identification or authentication. [AC-14]

6. Employ mechanisms to assist authorized users to determine whether access authorizations assigned to a sharing partner match the information's access and use restrictions. [AC-21]

7. Configure all Forest Service information systems to accept and electronically verify Personal Identity Verification-compliant credentials from other Federal agencies for authorized personnel where possible. [IA-2(12), IA-8(1)]

8. Accept only external authenticators that are NIST-compliant. In the system security plan, document and maintain a list of accepted external authenticators. [IA-8(2)]

6684.23 - Separation of Duties and Least Privilege

1. Restrict access to security systems and information to those personnel authorized to perform security related functions on the particular information system or equipment as defined in the system security plan. [AC-6(1)]

2. Grant users, or automated processes acting on behalf of users, the most restrictive rights, privileges, or access needed to perform assigned or specified tasks. Limit access to the resources that a user needs to complete or facilitate official duties. [AC-6(2)]

3. Configure the information system to enforce the concept of least privilege, allowing only authorized access for users (and processes acting on behalf of users) necessary to accomplish assigned tasks in accordance with organizational missions and business functions. [AC-6]

4. Ensure that only privileged user accounts or roles are used to perform functions that require elevated privileges. [AC-6(2), (5), (10)]

5. Separate duties of individuals such that no action can be taken without collusion.

6. Document separation of duties of individuals in the SSP in order that actions can be tracked and audited. [AC-5]

7. Define assigned information system access authorizations to support separation of duties. [AC-2a, AC-5]

8. Employ mechanisms to ensure the appropriate privileges are granted to system user credentials to prevent access beyond what is necessary to meet business mission. [AC-2-i, AC-6(7)]

6684.24 - Management of Generic and Guest Accounts

1. Create guest system access accounts only under the following conditions: [AC-2(9)]

a. The access is needed for conducting the Forest Service mission and an individually identifiable account access is impractical.

b. Network privileges for the guest or anonymous account only allow access to the public internet.

2. Create generic system access accounts, standing, managed accounts available for short-term use only under the following conditions: [AC-2(9)]

    a. The accounts are necessary for conducting the Forest Service mission.

    b. The accounts are centrally managed and documented.

    c. The accounts are assigned to one individual at a time and tracked in a way that definitively links use of the account to a specific individual.

    d. Passwords are changed immediately by the Manager of Generic System Access Accounts when the account is transferred to another user.

6684.25 - Public Access Protections

1. Configure all publicly available Forest Service information systems such that they protect the integrity and availability of the information and applications they support.

2. Employ only SSP-approved information system components to accept external credentials.

3. Identify and document all publicly accessible system components in the SSP.

4. Ensure that publicly accessible systems do not contain non-public information, including personally identifiable information.

6684.26 - Wireless Access Restrictions

1. Establish usage restrictions and implementation guidance for wireless access. [AC-18]

2. Continuously monitor for unauthorized wireless access. [SI-4]

3. Authorize wireless access to the information system prior to granting access and enforce requirements for wireless connections to the information system. [AC-18]

4. Disable wireless networking capabilities embedded within system components, when not intended for use, before issuance, and at deployment. [AC-18(3)]

6684.27 - Remote Access

1. Allow remote access to Forest Service networks only from Forest Service-issued devices or officially authorized personal devices using only documented and allowed methods. [AC-17]

2. Establish and document usage restrictions, configuration. connection requirements, and implementation guidance for each type of remote access in the system security plan. [AC-17]

2. Document all requests and resulting authorization for remote access using the Forest Service approved system for such documentation. [AC-17]

3. Prohibit the establishment of concurrent local area network, wide area network, and virtual private network (VPN) connections and/or dual connects/split tunneling. [SC-7(7)]

4. Revalidate the requirement for all users authorized for remote user access as required.

5. Deactivate, immediately, remote access accounts for users upon separation or determination that the access is no longer required.

6. Disable system functionality that provides the capability for automatic execution of code on mobile devices without user direction.

7. Use two-factor authentication for remote access and wireless access to both privileged and non-privileged accounts, and other Forest Service-approved methods. [AC-18(1)]

8. All remote session activity for both regular and security-related functions must be audited.

9. Allow all remote access, only through Forest Service approved encrypted Virtual Private Network (VPN) or equivalently secure, encrypted connections. [AC-17(2)]

10. Employ automated mechanisms to facilitate the information system monitoring and control of remote access on a continual basis. [AC-17(1)]

11. Control all remote accesses to a limited number of Forest Service-managed access control points. [AC-17(3)]

12. For access to privileged functions, permit such access only for compelling operational need, and document the rationale for such access in the information system SSP. [AC-6(3), AC-17(4)]

13. Other than the Internet connection required for the VPN connection to the Forest Service network, ensure that no other network connections, adapters, or communications ports, are active while the VPN session to the Forest Service network is active.

14. Ensure that desktop and laptop VPN configurations block access to all other networks, except access provided via the Forest Service network itself, while the VPN session to the Forest Service network is active.

15. When connecting a Forest Service computer (desktop or laptop) to a non-Forest Service public or home wired or wireless network,

    a. A VPN connection must be opened between the computer and the Forest Service Intranet immediately after connecting the computer to the non-Forest Service network unless connecting to a CIO-approved Forest Service system.

    b. Maintain that VPN connection in an active state for as long as the computer is connected to the non-Forest Service network.

    c. The Forest Service VPN connection must be used for all access to the public Internet.

16. For remote access, allow access only through Forest Service-approved connections.

    a. Manage all connections and remote access to Forest Service information systems centrally to ensure network integrity. [SI-4]

    b. Establish authentication procedures for remote users. [AC-18(1)]

    c. Locate virtual private network (VPN) services in a Forest Service-controlled DMZ, so that VPN traffic also must pass through perimeter firewalls.

    d. Configure remote access service to terminate connections automatically after a period of inactivity as specified in the applicable system security plan.

17. Remote access accounts or privileges will be immediately deactivated for anyone found to be in violation of this policy.

6684.28 - Access Control for Mobile Devices

1. Establish configuration requirements, connection requirements, and implementation guidance for mobile devices, including when mobile devices are outside of controlled areas. [AC-19a]

2. Authorize connection of mobile devices meeting organizational usage restrictions and implementation guidance to Forest Service information systems. [AC-19b]

3. Configure all Forest System-owned or -leased personal electronic devices:

    a. To automatically wipe (destroy) all information held on the device after unsuccessful login attempts as defined in the SSP, if possible. [AC-7(2)]

    b. To require the user to re-enter their password to regain access to the corporate information stored in the device when no interaction occurs between a user and the user's personal electronic device for a period of time, if the mobile device contains Forest Service corporate information (including email).

4. Remotely destroy all information held on Forest Service-owned or -leased personal electronic devices as soon as possible after they are reported as lost or stolen, to the extent possible.

5. Prohibit the use of unclassified mobile devices in facilities containing systems processing, storing, or transmitted classified information, unless specifically permitted by the authorizing official. [AC-19(4a)]

6. Enforce the following restrictions on individuals permitted by the authorizing official to use unclassified mobile devices in facilities containing systems processing, storing, or transmitting classified information: [AC-19(4b)]

    a. Prohibit the connection of unclassified mobile devices to classified systems.

    b. Obtain required approval from the authorizing official for connecting unclassified mobile devices to unclassified systems.

    c. Prohibit the use of internal or external modems or wireless interfaces within the unclassified mobile devices; and

    d. Conduct random reviews and inspections on unclassified mobile devices and the information stored on those devices, and if classified information is found, the incident handling policy is followed.

7. Restrict the connection of classified mobile devices to classified systems. [AC-19(4c)]

6684.29 - Use of External Systems and Publicly Accessible Content

1. The Forest Service establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems allowing authorized individuals to access

the information system from the external information system and process, store, and/or transmit organization-controlled information using the external information system. [AC-20]

2. The Forest Service restricts the use of Forest Service-controlled portable storage devices to only authorized individuals on external information systems. [AC-20(2)]

3. Retain approved information system connection or processing agreements with the organizational entity hosting the external information system. [AC-20(1)]

4. The Forest Service must be able to verify the implementation of the required security controls as specified in the Forest Service information security policy and security plan. [AC-20(1)]

5. The Forest Service designates individuals authorized to post information onto publicly accessible information systems. [AC-22]

6. Designated individuals will be trained to ensure that publicly accessible information does not contain non-public information. [AC-22]

7. All proposed content of publicly accessible information will be reviewed to ensure non-public information is removed prior to posting. [AC-22]

8. All content on publicly accessible information systems will be reviewed periodically and non-public information will be removed, if discovered. [AC-22]

6684.3 - Security Monitoring/Audit Controls

1. Employ mechanisms to continuously monitor and review user activity on Forest Service information systems and networks.

2. Investigate unusual information system related activities.

3. Regularly scan or otherwise monitor Forest Service endpoints (desktop and laptop computers) to detect the presence of unauthorized software and take appropriate action to remove or mitigate.

4. Continuously monitor Forest Service networks and computer activity to detect, report, disable, and/or cause the repair, removal, or mitigation of:

    a. Intrusions by or the presence of malware (computer viruses, worms, or Trojans), spyware, or other unauthorized software that attempts to install itself and operate on Forest Service networks or computers without Forest Service authorization.

b. Unauthorized access to internal or external network or computing devices.

c. Unsolicited or offensive electronic messaging content that violates Forest Service policy on appropriate use of IT resources.

d. Known vulnerabilities in the software or hardware configurations of Forest Service-owned or operated IT.

5. Use data collected through security monitoring only to:

   a. Assist the Forest Service in achieving audit compliance.

   b. Monitor service levels.

   c. Support official administrative or criminal investigations.

   d. Limit Forest Service liability.

   e. Measure system and network performance.

   f. Perform system and network capacity planning activities.

   g. Troubleshoot system and network problems.

   h. Safeguard the confidentiality, integrity, and availability of corporate information and protect information systems, networks, and users from inappropriate or unauthorized use.

6. Use automated monitoring tools when they provide exception based, real time notification of threats, vulnerability exploitations, and unauthorized or inappropriate system or network usage detected by monitoring:

   a. Traffic originating from or destined for the Internet.

   b. Electronic messaging traffic (including, but not limited to, electronic mail, instant messaging, and mobile communication device text messaging) received by or sent from Forest Service information systems.

   c. Forest Service intranet, local area, and wide area network traffic, and protocols.

   d. Operating system and other system software security indicators, including system activity logs, on Forest Service-owned or operated IT.

7. Perform the following actions for data collected to meet system monitoring requirements, regardless of whether it contains personally identifying information:

a. Allow the collection and analysis of data in its raw state only by System Administrators, security personnel, or their Managers in the authorized performance of their official duties.

b. Treat the data as confidential and reveal the data to others only pursuant to legal, regulatory, or investigatory requirements, and in a redacted format omitting any personally identifying information, unless or until the data becomes part of an authorized investigation.

c. Immediately report evidence of suspected or alleged misconduct discovered through routine system monitoring in accordance with departmental and Forest Service procedures regarding investigation of employee misconduct.

d. Destroy the data immediately once the administrative need or legal requirement for its retention has expired.

8. Provide annual notification to employees regarding security monitoring activities, privacy expectations, and appropriate use.

6684.31 - Audit Events

1. Ensure information systems audit and produce records for the events and privileged functions identified in the system's SSP. [AC-6(9)]

2. Provide the capability for audit reduction and audit report generation. [AU-7]

3. Review and update the list of defined auditable events at least periodically. [AU-2]

4. Secure all audit logs, in accordance with Federal guidance. [AU-9]

5. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events. [AU-2]

6. Analyze and correlate audit records across mission areas, business process levels and system levels. [AU-6(3)]

6684.32 - Content of Audit Records

1. For audit events, collect adequate information to investigate security incidents, including, but not limited to, the type of event, when the event occurred, where the event occurred, source, and outcome of the event. [AU-3, AU-3(1)]

2. Limit the PII contained in audit records to the system's privacy risk assessment. [AU-3(3) PRIV]

3. Show time/date of user logon and logoff, and the workstation internet protocol (IP) address, name, or identifier of the location used. [AU-3(1)]

4. Record the unique identifier; the workstation IP address, name, or identifier of the location used to initiate the action; the function or file operation being performed; the time and date of all server system administration functions and file operations; and the outcome (success or failure) of the event. [AU-3(1)]

5. Show the use of individual system communication ports, if practical and applicable. [AU-3(1)]

6. Record every invalid attempt to logon to applications, systems, or networks, along with time/date of attempt, and the workstation IP address, name, or identifier of the location used to attempt logon, if available. [AU-3(1)]

6684.33 - Response to Audit Processing Failures and Audit Record Review, Analysis, and Reporting and Audit Record Reduction and Report Generation

1. Review and analyze information system audit records, or as identified in the SSP, for indications of inappropriate or unusual activity. [AU-6]

2. Investigate suspicious activity or suspected violations and report findings. [AU-6]

3. Employ automated mechanisms to alert security personnel of inappropriate or unusual activities with security implications, for audit events. [AU-6]

4. Configure information systems to:

    a. Alert designated Forest Service officials in the event of an audit processing failure and take corrective action. [AU-5]

    b. Overwrite the oldest audit records in the event of audit log overflow.

    c. Provide an audit reduction and report generation capability that supports on-demand audit review, analysis, and reporting requirements and after-the-fact investigations of security incident. [AU-7]

    d. Provide an audit reduction and report generation capability that does not alter the original content or time ordering of audit records. [AU-7]

    e. Provide the capability to review and analyze audit records for events of interest based on specific audit fields within audit records. [AU-6]

f. For audit events, provide information capable of supporting an after the fact investigation of an event as defined in the system security plan to system management. [AU-6]

5. Adjust the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. [AU-6]

6. Integrate audit record review, analysis, and reporting across Forest Service processes for incident response, continuous monitoring, contingency planning, audits, and response to suspicious activities. [AU-6(1)]

6684.34 - Time Stamps

1. For audit events: [AU-8]

    a. Configure the information system to generate time stamps for use in audit record generation.

    b. Show time/date of user logon and logoff and the workstation IP address, name, or identifier of the location used.

2. Ensure all systems synchronize to a USDA- or Forest Service-authorized time source (such as Greenwich Mean Time source). [AU-8, SC-45(1)]

3. Ensure the time stamps are generated using internal IT system clocks that are synchronized daily at a minimum enterprise wide. [AU-8]

4. Use internal system clocks to generate time stamps for audit records. [AU-8]

6684.35 - Protection of Audit Information

1. Configure IT systems to protect all audit information and audit tools from actions such as unauthorized access, modification, and destruction. [AU-9]

2. Alert system owners and ISSOs to unauthorized access, modification, or deletion of audit information. [AU-9]

3. Permit only authorized personnel to have access to the audit logs and audit tools. [AU-9(4)]

6684.36 - Audit Log Storage Capacity and Record Retention

1. Ensure the information system allocates adequate audit record storage capacity. [AU-4]

2. Retain system, application, and database-level audit logs for a minimum period of time online as defined in the SSP and for after-the-fact investigations of IT security incidents. [AU-11]

    a. Ensure the most recent records of activity as defined in the SSP are readily accessible at all times; use a longer period if needed to support requirements of a particular information system.

    b. Ensure that all audit records are retained in accordance with official records management and retention requirements and applicable litigation requirements.

6684.37 - Audit Record Generation

1. The information system provides audit record generation capability for the identified audit events, capable of creating audit records as defined in the system security plan and processing, sorting, and searching audit records for events of interest.
[AU-2, AU-12, AU-7(1)]

2. The information system allows designated Forest Service personnel to select which audit events are to be audited by specific information system components. [AU-12]

3. The information system generates audit records for the list of identified audit events. [AU-2, AU-3, AU-12]

6684.4 - System and Communications Protections

6684.41 - Mobile Code

1. Define acceptable and unacceptable mobile code and mobile code technologies. [SC-18]

2. Establish usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies.

3. Authorize, monitor, and control the use of mobile code within the information system. [SC-18]

6684.42 - Use of Cryptography

1. If cryptography is used, establish, and manage cryptographic keys for required cryptography employed within the information system as documented in the SSP. This should include the correct type of cryptographic for each use and the requirements for key generation, distribution, storage, access, and destruction. [SC-12, SC-13]

2. Ensure cryptographic mechanisms for authentication are compliant with the current version of FIPS 140, applicable Federal laws, Executive Orders, directives, policies, regulations, standards and are approved by the department. [IA-7]

3. Issue public key infrastructure (PKI) certificates under an agency certificate authority or an approved PKI service provider. Include only approved trust anchors in trust stores or certificate stores managed by the organization. [SC-17]

4. Whole disk encryption is to be utilized on all portable Forest Service computers. [AC-19(5)]

6684.43 - Process Isolation

Maintain a separate execution domain for each executing process within the information system. [SC-39]

6684.5 - Device Identification and Authentication

1. Configure information systems to uniquely identify and authenticate specific devices before establishing connection. [IA-3]

2. Verify that only approved procedures, mechanisms, or protocols are used for host or device authentication.

3. Document with clarity, in the SSP, the procedures, mechanisms, or protocols used for device authentication, including diagrams.

4. Implement device authentication controls mechanisms in keeping with the current version of FIPS 199 security categorization of the information system. [IA-5(6)]

6684.6 - Network Security

6684.61 - Voice over Internet Protocol

1. Implement Voice over Internet Protocol (VoIP) only through usage restrictions based on the potential to cause damage to the information system if used maliciously and only when the use is authorized, monitored, and controlled.

2. Authorize, monitor, and control the use of VoIP within the information system.

3. Limit access, including remote access, to the management features of any electronic network infrastructure equipment owned and/or managed by the Forest Service to specifically authorized individuals.

6684.62 - Boundary Protection and System Partitioning

1. Monitor and control communications at the external boundary of the Forest Service network and at key internal boundaries within the Forest Service network. [SC-7]

2. Implement subnetworks for publicly accessible system components that are separated from internal organizational networks. [SC-7]

    a. Allow Internet access from Forest Service networks only through the managed interfaces provided by the U.S. Department of Agriculture (USDA) approved Internet access nodes.

    b. Allow public Internet access to Forest Service information systems by implementing subnetworks for publicly accessible servers, creating a demilitarized zone (DMZ) controlled by the Forest Service or otherwise isolated from Forest Service networks. Do not place servers that are directly accessible by entities on the public Internet, including Web servers, inside the Forest Service intranet.

3. Connect to external networks or systems only through managed interfaces consisting of boundary protection devices. [SC-7]

4. Limit the number of external network connections. [SC-7(3)]

5. Protect the authenticity of all communications sessions. [SC-23]

6. Activate network services only as required to meet the Forest Service mission.

    a. Remove or deactivate all services on all servers that are not needed or not approved for use.

    b. Document in the system security plan any services allowed to pass through Forest Service network security controls, including a description of the service, ports used, reason the exception is required, and associated security controls.

    c. Prevent remote devices and services that have established a non-remote connection with the system from communicating outside of that

communications path with resources in external networks (for example, split-tunneling technologies are prohibited).

7. Implement network-based security tools designed to notify System Administrators of unauthorized access or attempted access to Forest Service networks and, if possible, configured to prevent such access through automated interaction with perimeter firewalls or other security controls.

8. Partition the information system into components residing in separate physical domains or environments as necessary.

9. Select security features and mechanisms to provide defense in depth through management of internal activities and external connections.

    a. See exhibit 01, for direction on requirements for configuring internal and external devices.

    b. See exhibit 02, for direction on configuring perimeter security device filtering rules.

6684.62 - Exhibit 01

Configuring Internal and External Devices

1. Full content network traffic is visible to a sensor.

2. Virtual private networks (VPN) traffic terminates where the traffic may be processed by a Network Intrusion Detection System, Host-based Intrusion Detection System or Intrusion Prevention System and does not bypass the security architecture.

3. Allow changes to perimeter firewalls only when authorized by the USDA, OCIO or designated representative.

4. Document all permitted IP addresses and ports.

5. VPN communications to or from the network to employ, at a minimum, a current version of FIPS 140-2 approved data encryption module (for example, Advanced Encryption Standard [AES]).

6. Perimeter security devices maintain a separate access password.

7. Design and configure information systems to protect against or limit the effects of denial-of-service attacks. [SC-5]

8. Monitor and log the operation of network perimeter security systems to the extent necessary to substantiate investigations of real or perceived security violations. At a minimum, record client transaction information such as source and destination IP address, date and time, port used or requested, and uniform resource locator, if available.

9. Maintain components responsible for monitoring and ensuring network security, including but not limited to routers, firewalls, intrusion detection/prevention systems, spam and antivirus filters, and vulnerability scanning systems, as follows:

    a. Update or patch network security components as recommended by the manufacturer.

    b. Test changes to network security components, including reconfigurations, updates, or patches, offline whenever possible, before placing them into production status.

10. Implement a managed interface for each external telecommunication service. [SC-7(4)]

11. Control the flow of information within the information system(s) and between interconnected information system(s). [SC-7(4)]

12. Protect the confidentiality and integrity of the information being transmitted across each interface. [SC-7(4)], [SC-8]

13. Document each exception to the traffic flow policy with a supporting mission/business need and the duration of that need. Review the exceptions to the traffic flow policy periodically. Remove the traffic flow policy exemptions that are no longer supported. [SC-7(4)]

14. Prevent unauthorized exchange of control plane traffic with external networks, publish information to enable remote networks to detect unauthorized control plan traffic from internal networks, and filter unauthorized control plan traffic from external networks. [SC-7(24) PRIV]

15. Ensure the information system at the managed interfaces denies network traffic by default and allows network traffic by exception (for example, deny all, permit by exception). [SC-7(5)]

6684.62 - Exhibit 02

Configuring Perimeter Security Devices Filtering Rules

1. Packets coming from an external source into the IT system do not have a source address of the IT system's internal network.

2. Packets leaving the internal network do not have a destination address of the IT system's internal network.

3. Packets coming into the IT system from the Internet or leaving the IT system's network to the Internet do not have a private source or destination address or an IP address listed in Request for Comments (RFC) RFC1918 reserved space. All packets reference only the IT system's external public IP address.

4. As applicable, block any source routed packets or any packets with IP options that are not specifically allowed (for example, multicast, IP Security [IPSEC], and so forth.).

5. Actively manage devices that are connected to the Forest Service network, and all Forest Service provided services available via the network to ensure the integrity, performance, and availability of the network and network services.

6. Route traffic through authenticated proxy servers at managed interfaces. [SC-7(8)]

7. Locate Web servers and information that are accessible to the general public on a screened subnet, such as a DMZ that is protected by a firewall that is enabled to be accessed by external Internet clients. The DMZ may also contain other servers, such as mail servers, remote access machines, or Web servers.

8. Identify and document the defined boundary of the information system in the SSP and RA.

9. Implement Information Exchange Security Agreements (IESAs) or Memorandum of Understanding/Agreements (MOU/As for IT systems with connections that are external to the Forest Service.

10. Conduct periodic testing of incoming perimeter filtering protection mechanisms.

6684.63 - Secure Name/Address Resolution Service

1. Configure all information system servers that provide name/address resolution in accordance with current guidance and available USDA Secure Name/Address Resolution capabilities.

2. Implement appropriate system and network security controls for securing the Domain Name System (DNS) hosting environment, such as operating system and application patching, process isolation, and network fault tolerance.

3. Provide additional data origin authentication and integrity verification artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries. [SC-20]

4. Configure the information system, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains. [SC-20]

5. Configure the information system to request and perform data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources. [SC-21]

6. Ensure the systems that collectively provide name/address resolution service are fault-tolerant and implement internal and external role separation. [SC-22]

7. Protect DNS transactions such as update of DNS name resolution data and data replication that involve DNS node. The transactions should be protected using appropriate cryptographic methods, including hash-based message authentication codes based on shared secrets and/or digital signatures. [SC-8(1)]

6684.64 - Transmission Confidentiality and Integrity

1. Protect the integrity and confidentiality of transmitted information when that information traverses' external connections by employing cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures. [SC-8(1)]

2. Require transmission integrity and confidentiality controls in contracting vehicles and agreements for external connections.

3. When using commercial service providers that lack transmission integrity and confidentiality service level agreements, use transport integrity and confidentiality security mechanisms that are in accordance with current guidance from NIST and Committee on National Security Systems (CNSS) Instruction No. 7003, "Protected

Distribution Systems (PDS)", regarding Transport Layer Security, IPsec, and Domain Name Systems.

4. Implement appropriate compensating security controls on any systems transmitting information that traverse external connections without protecting the integrity and confidentiality of the information transmitted or accept and document the additional risk incurred.

6684.65 - Network Disconnect and Session Authenticity

1. Ensure the system protects the confidentiality and integrity of data at rest. [SC-28]

2. Configure the information system to terminate the network connection associated with a communications session at the end of the session or after periods of inactivity as defined in the SSP. [SC-10]

6684.7 - Information in Shared System Resources

1. Configure all information systems to prevent unauthorized and unintended information transfer via shared system resources. [SC-4]

2. For systems that process PII, monitor permitted processing rules for data elements of PII, document each exception, and review and remove exceptions that are no longer supported. [SC-7(24]

3. Activate the security system's object reuse function.

4. Ensure that unauthorized access to a user's residual data cannot be obtained.

5. Ensure that any previous information content of the system is made unavailable upon the allocation of the resource to all subjects.

6. Render all storage devices unreadable only by degaussing or overwriting in accordance with Information Technology Security Requirements for Media Protection.

7. Enforce or execute the deletion of temporary files created.

8. Clear, purge, or destroy all computers, disk drives, printers, copiers, scanners, and so forth upon removal from the general support system.

9. Configure all systems not to default to core dumps when the system fails.

10. Ensure the information system separates user functionality (including user interface services) from information system management functionality. [SC-2]

6684.8 - Additional Security Technical Controls for High Value Asset Systems

Note: These policies only apply to information systems designated by USDA as a High Value Asset (HVA) System.

6684.8a - Access Enforcement

Release information outside of the Forest Service information system only if the receiving system or system component provides adequate security and privacy controls and the system or system components have been validated. [AC-3(9)]

6684.8b - Audit Record Review, Analysis, and Reporting

1. Provide and implement the capability to centrally review and analyze audit records from multiple components of an information system. [AU-6(4)]

2. Integrate the analysis of audit records with analysis of information generated by scanning, monitoring, or other data collection activities. [AU-6(5)]

6684.8c - Protection of Audit Information

1. Store audit records in a repository that is part of physically different system or system component than the system or component being audited. [AU-9(2)]

2. Implement cryptographic mechanisms to protect the integrity of audit information and audit tools. [AU-9(3)]

3. Authorize access to management of audit logging functionality to only authorized privileged access personnel. [AU-9(4)]

4. Enforce dual authorization for movement or deletion of audit information. [AU-9(5)]

5. Authorize read-only access to audit information to authorized privileged access personnel. [AU-9(6)]

6684.8d - Non-Repudiation

Provide irrefutable evidence that an individual or process acting on behalf of an individual has performed any audit actions. [AU-10]

6684.8e - Cross Organization Audit Logging

Coordinate audit information among external organizations when audit information is transmitted across organizational boundaries. [AU-16]

6684.8f - Security Function Isolation

Isolate security functions, including enforcing access and information flow control from nonsecurity functions and other security functions, by implementing partitions and domains. [SC-3, 3(2)]

6684.8g - Denial-of-Service Protection

1. Protect against the effects of denials-of-service [SC-5]

2. Restrict the ability of individuals to launch denial-of-service attacks against other systems. [SC-5(1)]

3. Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding denial-of-service attacks. [SC-5(2)]

4. Employ tools to detect indicators of denial-of-service attacks against or launched from a Forest Service information system. [SC-5(3)]

5. Monitor system resources to determine if sufficient resources exist to prevent effective denial-of-service attacks. [SC-5(3)]

6684.8h - Boundary Protection

1. Prevent the exfiltration of information and conduct exfiltration tests. [SC-7(10)]

2. Allow only incoming communications from authorized sources to be routed to authorized destinations. [SC-7(11)]

3. Implement boundary protection at system components. [SC-7(12)]

4. Protect against unauthorized physical connections at managed interfaces. [SC-7(14)]

5. Enforce adherence to protocol formats, [SC-7(17)]

6. Employ boundary protection to isolate system components supporting mission or business functions. [SC-7(21)]

6684.8i - Mobile Code

Prevent the automatic execution of mobile code in software applications and enforce actions like prompting users prior to executing the code. [SC-18(4)]

6685 - Privacy Controls

6685.01 - Authority

6685.01a - Laws

6685.02 - Objectives

To implement privacy controls focused on the management of risk and the management of information system security for information technology (IT) resources that support the Forest Service mission.

Assure individuals, from whom information is collected, that:

1. The Forest Service does not use any personal recordkeeping systems whose very existence are secret.

2. The Forest Service personal information file access is limited to those with "need to know."

3. The individuals will have an opportunity to inspect their saved information and to challenge its accuracy.

4. Personal information collected for one purpose may not be used for another purpose without their consent.

5. If disclosures are made, the individuals will learn to whom they were made, for what purpose, and on what date.

6685.03 - Policy [Reserved]

6685.04 - Responsibility

6685.04a - Assistant Chief Information Officer for Natural Resources and Environment

The Assistant Chief Information Officer (ACIO) for NRE is responsible for:

1. Managing risk related to Forest Service information systems, including establishing an enterprise Risk Assessment (RA) program and ensuring adequate resources are allocated for the continuing assessment and mitigation of information privacy risks.

2. Formally designating a Forest Service Systems Privacy Officer to oversee all privacy-related information security issues.

3. Ensuring that Privacy Threshold Analysis (PTA) and applicable Privacy Impact Assessments (PIAs) are conducted and submitted to appropriate authorities in accordance with U.S. Department of Agriculture (USDA), Office of Management and Budget (OMB), and Forest Service policy (including the privacy provisions of Section 208 of the E-Government Act and of the Privacy Act of 1974).

4. Acting as the Senior Agency Officer for Privacy (SAOP) with the overall responsibility and accountability for ensuring the Forest Service's implementation of information privacy protections, including: the Forest Service's full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act; management of the development, documentation, and dissemination of the PII processing and transparency policy and procedures. [PT-1(b)].

5. Allocating sufficient Forest Service resources to implement and operate Forest Service-wide privacy program.

6. Ensuring compliance with requirements for immediate and long-term training needs in support of privacy requirements.

7. Ensuring compliance with requirements for protecting the confidentiality and integrity of personally identifiable information (PII).

8. Overseeing the development, dissemination, and updates of reports to the OMB, Congress, and other oversight bodies, as appropriate to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management.

9. Establishing a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. When applicable, computer matching agreements will be published on a publicly accessible Website.

6685.04b - Assistant Chief Information Security Officer for NRE

The Assistant Chief Information Security Officer (ACISO) for NRE is responsible for:

1. Supporting the Forest Service Risk Management Program by developing and implementing Forest Service-wide policies and procedures for assessing privacy security risks.

2. Implementing a Forest Service-wide security and privacy assessment and authorization process. Assisting with security and privacy assessment and authorization activities.

3. Limiting the use of PII in testing, training, and research efforts.

4. Disseminating this policy to all IT professionals, security officers, and system owners who will be involved in the security and privacy assessment and authorization process to ensure they understand and can fulfill their roles and responsibilities.

5. Ensuring that privacy practices are publicly available through organizational websites, and that the public has access to information about privacy activities and is able to communicate with Senior Agency Officials for Privacy (SAOP)/Chief Privacy Officers.

6685.04c - Information System Security Manager

Information System Security Managers are responsible for:

1. Supporting the Forest Service system security and privacy plan by verifying that all systems security plans are submitted to the ACIO and the Authorizing Official (AO).

2. Implementing a Forest Service-wide security and privacy assessment and authorization process.

3. Assisting with security and privacy assessment and authorization activities.

6685.04d - Systems Privacy Officer

The Systems Privacy Officer is responsible for:

1. Ensuring that Forest Service information systems or services comply with applicable privacy laws, regulations, and USDA and Forest Service policies for protecting the confidentiality of PII.

2. Ensuring that the privacy implications to individuals of new information systems or services are determined before development begins, and that a PIA is conducted as required by USDA Departmental Manual (DM) 3515-002.

3. Serving as the primary point of contact for all privacy-related information security issues.

4. Communicating a comprehensive Forest Service-wide Privacy Program.

5. Issuing guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information.

6. Establishing privacy roles, responsibilities, and access requirements for contractors and service providers.

7. Coordinating with the system developer to resolve questions during the PTA process.

8. Inspecting existing systems to determine whether a PIA is needed, and subsequently requiring a PIA, System of Records Notice (SORN) or both for existing systems when deemed necessary.

9. Furthering all PIA oriented efforts through planning for new processes and procedures.

10. Conducting investigations where a suspected breach of privacy information is involved.

11. Developing or overseeing the development of privacy related training and awareness materials.

12. Conducting privacy related training as required.

13. Conducting compliance reviews to ensure all Forest Service information systems have conducted a PIA and SORNs, as required.

14. Reviewing the use of social security numbers (SSNs) within Forest Service operational systems and programs to identify instances where the collection or usage is not necessary and can be eliminated.

15. Ensuring data about the public that the Forest Service maintains is accurate, relevant, timely, and complete.

16. Identifying the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection and limiting the collection of information to the minimum elements identified.

17. Coordinating with the Forest Service Forms Manager and Webmaster to ensure that all public use forms, surveys, or non-forms (collections of standardized information on the Internet) contain instructions, the OMB approved information collection control number, burden disclaimer statement, and the expiration date, unless otherwise requested.

18. Coordinating with the Forest Service Privacy Act Officer to complete Privacy Threshold Analyses and Privacy Impact Assessments; and grant exceptions.

19. Collaborating with the Privacy Act Officer to provide guidance on safeguarding the disclosures of public personal data in strict accordance with the Privacy Act.

20. Monitoring Federal privacy laws and policy for changes that affect the Privacy Program.

21. Ensuring that public notices are modified, issued, and disseminated to reflect changes in practice or policy that affect PII or changes in activities that impact privacy, before or as soon as practicable after the change.

22. Ensuring that risk determination is conducted as required by system owners as part of the Risk Assessment (RA) updating process, including RA updates as part of PIA updates.

23. Reviewing adherence to security and privacy control requirements related to protecting the confidentiality and integrity of PII.

24. Overseeing the monitoring and auditing of privacy controls and internal privacy policy to ensure effective implementation of the Forest Service Privacy Program.

25. Implementing an Agency-wide security and privacy assessment and authorization process in accordance with FSM 6682.4 and assisting with security and privacy assessment and authorization activities.

6685.04e - Office of Regulatory and Management Services Director

The Office of Records and Management Services (ORMS) Director is responsible for:

1. Communicating compliance requirements for protecting the confidentiality and integrity of personally identifiable information (PII).

2. Providing guidance to the Agency regarding Privacy Act standards to manage content that meets regulatory, Department and Forest Service priorities.

3. Maintaining a consolidated list of all programs and information systems identified as collecting, using, maintaining, or sharing PII, based on information provided by the Systems Privacy Officer, Records Manager, and Forms Manager.

4. Maintaining a current list of Privacy Act System of Record Notices describing programs and information systems identified as collecting, using, maintaining, or sharing PII; note that the System Owner is responsible for updating the System of Record Notice.

6685.04f - Forms Manager's Supervisor

The Forms Manager's Supervisor is responsible for verifying the National Form Manager coordination with form sponsors to properly develop forms, assure PII is securely collected by coordinating with the Directives and Regulations unit, meet CIO requirements, and maintain an updated forms SharePoint site to ensure that all public use forms, surveys, or non-forms (collections of standardized information on the Internet) contain instructions.

6685.04g - Forms Manager

The Forms Manager is responsible for coordination with form sponsors to properly develop forms, assure PII is securely collected by coordinating with the Directives and Regulations unit, meet CIO requirements, and maintain an updated form SharePoint site to ensure that all public use forms, surveys, or non-forms (collections of standardized information on the Internet) contain instructions

6685.04h - Forest Service Information Collection Officer

The Forest Service Information Collection Officer (ICO) is responsible for coordination with sponsors that are obtaining or soliciting facts or opinions posed to 10 or more persons from a non-Federal entity through written reports, application forms, schedules, or questionnaires with identical questions (oral, written or electronic), whether voluntary or mandatory. The ICO will assist a system owner or sponsor with properly filling out an Office of Management and Budget (OMB) information collection request, and a Federal Register Notice.

6685.04i - National Records Manager's Supervisor

The National Records Manager's Supervisor is responsible for monitoring employees and contractors who safeguard the public's personal data to ensure that all disclosures are made with an individual's written permission or are made in strict accordance with the Privacy Act.

6685.04j - Forest Service Records Officer

The Forest Service Records Officer is responsible for:

1. Working with the Systems Privacy Officer and system proponents to ensure that National Archives and Records Administration (NARA) -approved records retention schedules are established for unstructured and structured data, including (but not limited to) data in proposed and existing relational databases.

2. Fulfilling assigned records management program management responsibilities as set forth in Forest Service Manual (FSM) 6230, Records Management and Forest Service Handbook (FSH) 6209.11, Records Management Handbook.

3. Assisting Program Managers or Specialists by providing training, technical assistance, and guidance in preparing information collection requests to keep public burden to a minimum.

4. Verifying the Agency retains an individual's personal information only as long as necessary to fulfill the purposes for which it is collected and that records are destroyed in accordance with established Federal, USDA, or Forest Service records management schedules.

6685.04k - Freedom of Information Act/Privacy Act Assistant Director

The Freedom of Information Act (FOIA)/Privacy Act Assistant Director is responsible for:

1. Upholding legal guidance determining which records must be made available to a requester and which records can be withheld.

2. Providing administrative and judicial remedies for those denied access to records.

3. Providing the fullest possible disclosure of information to the public.

4. Leveraging technology to ensure general program information and disclosed information are accessible to the extent possible.

5. Maintaining an electronic reading room that includes Forest Service policies; staff manuals; opinions made in the adjudication of cases; and records sets released under FOIA that are likely to become the subject of subsequent FOIA requests.

6. Documenting in a SORN: agency authority to collect Personally Identifiable Information and the purpose of a system's collection; how Personally Identifiable Information is used; and individual rights to access, review, and make requests to correct and/or update that individual's information.

7. Providing guidance for system owners to monitor/verify employees and contractors responsible for safeguarding the public's personal data ensure that disclosures are made in strict accordance with the Privacy Act.

6685.04l - Privacy Act Officer

The Privacy Act Officer is responsible for:

1. Ensuring that SORNs are created/updated and approved through appropriate Forest Service and USDA authorities; or are removed in accordance with USDA, Office of Management and Budget (OMB), and Forest Service policy (including the privacy provisions of Section 208 of the eGovernment Act and of the Privacy Act of 1974).

2. Verifying that, unless exempt from the Privacy Act, the Forest Service will, upon request, grant an individual access to that individual's records; provide the individual a list of disclosures made outside the Forest Service, and correct that individual's file when shown to be in error.

4. Ensuring that Forest Service adheres to requirements set forth in the Privacy Act, USDA privacy regulations; OMB privacy policies, and Forest Service Manual (FSM) 6270, Availability of Records.

5. Provide guidance so that individuals can access, review, and request updates to information. Guidance must include the process for accessing SORN.

6. Maintaining an accurate accounting of disclosures of information held in each system of records under Forest Service control and retain the accounting of disclosures.

6685.04m - Authorizing Official

The Authorizing Official (AO) is responsible for:

1. Conducting privacy assessments in accordance with the current USDA privacy policies and other current Federal, Departmental, and Forest Service regulations.

2. Approving privacy requirements, deviations from privacy policies (as agreed with the Contracting Officer (CO) and Forest Service (ACISO), and memoranda of agreement or understanding.

3. Approving systems that contain PII only after they have implemented the appropriate controls. Systems using PII are used within the organization. If PII must be shared outside the organization, enter into appropriate agreements (for example, Information

   Exchange Security Agreements, Memorandum of Understandings) to protect Privacy Information. Use of PII is only permitted for the authorized purposes identified in the Privacy Act and/or described in notice(s) or for a purpose that is compatible with those purposes.

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

6685.04n - System Owners

The system owner is responsible for the following for each of their assigned systems:

1. Incorporating privacy requirements and controls into the System Development Life Cycle (SDLC).

2. Developing, implementing, and maintaining a system security plan (SSP) for each of their information systems with guidance found in NIST SP 800-18 Rev. 1 and FSM 6680.

3. Minimizing risk to the Forest Service IT infrastructure, including PII and corporate data in the development, testing, and maintenance of the system and applications.

4. Providing sufficient resources to:

    a. Ensure that system users and security support personnel obtain required role-based security and privacy training which requires users certify acceptance of responsibilities.

    b. Comply with requirements to protect the confidentiality of any PII collected and/or retained by their system.

    c. Review all Privacy Act exemptions claimed for the system of records, to ensure they remain appropriate and necessary.

5. Ensuring that all IT privacy controls in the information systems are monitored on an ongoing basis.

6. Minimizing the use of PII for testing, training, and research. Implementing controls to protect PII when used for testing, training, and research and where feasible, use techniques to minimize the risk.

7. Preparing PTAs, PIAs and SORNs. Ensuring SORNs are current and up to date. Removing SORNS when they are no longer needed.

8. Ensuring that the Risk Assessment for the information system is updated as part of the IT system's continuous monitoring of privacy controls, or as needed.

9. Preparing any required new, amended, or altered systems notices for the system of records and submit them through the Forest Service Privacy Officer and Privacy Act Officer for publication in the Federal Register.

10. Providing procedures for individuals to authorize the collection, use, maintenance, and sharing of PII prior to its collection.

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

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

13. Ensuring for non-archived holdings of all PII, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete, and reducing them to the minimum necessary for the proper performance of a documented Forest Service function.

14. Ensuring no official files on individuals are retrieved by name or other personal identifier without first ensuring that a notice of the system of records has been published in the Federal Register.

15. Ensuring that all personnel who either have access to the system of records or who develop or supervise procedures for handling records in the system of records are aware of their responsibilities for protecting personal information being collected and maintained.

16. Ensuring that all systems maintain accurate, relevant, timely, and complete data about the public.

17. Reviewing non-archived holdings of all PII and ensuring, to the maximum extent practicable, such holdings are accurate, relevant, timely, complete, and reducing them to the minimum necessary for the proper performance of a documented Forest Service function.

18. Reviewing the use of social security numbers in agency operational systems and programs to identify instances in which collection or use of the social security number is not required. Submitting a waiver to the Department for authorization to collect SSN when required.

19. Establishing, and documenting in the security authorization package, interconnection agreements with other systems that specify privacy controls and responsibilities for the interconnected systems.

20. Monitoring, auditing, and making system staff aware about the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing.

21. Deciding who should have access to the PII information and what their system privileges or access rights should be.

22. Assisting in the identification and assessment of the common privacy controls where the information resides.

23. Collecting and retaining PII in compliance with FSM 1380.3. Conducting an initial evaluation of PII holdings and review those holdings to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. Complying with the requirement for annual reviews of PII retained by information systems.

24. Coordinating with an (Office of Records and Management Services (ORMS) Information Collection Officer for the establishment or renewal of an Information Collection Instrument, in addition to the preparation of the 60-day Federal Register notice, prior to the expiration of an existing collection instrument, or desired "use date" of a new collection instrument.

25. Verifying when the Agency collects personal data, all members of the public are informed of the intended uses of the data, the disclosures that will be made, the authorities for the collection, and whether the collection is mandatory or voluntary.

26. Maintaining all records which are used by the Forest Service in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.

27. Establishing appropriate administrative, technical, and physical safeguards to ensure the privacy of records and to protect against any anticipated threats or hazards to their security, personal information or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

28. Using Forest Service methods to dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access. See FSH 6209.11, Chapters 30 and 40 for details; consult assigned Records Manager or Forest Service Records Officer as needed.

29. Monitoring employees and contractors who safeguard the public's personal data to ensure that all disclosures are made with an individual's written permission or are made in strict accordance with the Privacy Act.

30. Incorporating the System Privacy Plan into the System Security Plan (SSP) unless otherwise directed.

6685.04o - Information System Security Officer

Each Information System Security Officer is responsible for the following in each system to which they are assigned:

1. Reviewing and validating system privacy controls as scheduled by USDA to ensure they are in place and operating as intended.

2. Assessing system changes to evaluate if updates will create a new privacy risk.

3. Assisting in creation of, updates to, or deletion of system PTAs, PIAs, and SORNs and coordinating with the System Privacy Officer and Forest Service Privacy Act Officer, as well as ORMS.

4. Monitoring the day-to-day security of systems, including physical and logical authorization and access, incident response, compliance with requirements for protecting the confidentiality of PII, and awareness training and education.

5. Performing monitoring and auditing of privacy controls that apply to the systems they are assigned.

6. Monitoring internal privacy policy to ensure effective implementation of the Forest Service Privacy Program.

6685.04p - Information System or Application Program Managers and Application Developers

Information System or Application Program Managers and Application Developers are responsible for:

1. Designing information systems to implement privacy controls based on the security categorization of the system and the confidentiality impact level of any PII collected and/or retained by the system.

2. Designing into any application the privacy controls required by the current version of NIST SP 800-53, and those privacy controls necessary to minimize the need for separation of duties.

3. Designing information systems to employ technologies and system capabilities that automate privacy controls. Implementing mechanisms to support itemized or tiered consent for specific uses of data.

4. Configuring information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule (see FSH 6209.11, Ch. 40 or contact Forest Service Records Officer for information on approved record retention schedules for information systems).

5. Operating, maintaining, and disposing of their systems in accordance with the security plans and other documented privacy control requirements in conjunction with the system owner.

6. Ensuring that the systems they manage provide required security and PII awareness training for system users and security support personnel.

7. Participating in PTA and PIA activities.

6685.04q - Procurement and Property Services and Grants and Agreements Personnel

Forest Service Contracting Officers, Purchasing Agents, Grants Management Specialists, and Real Property Leasing Officers are responsible for:

1. Requiring contractor or cooperator compliance with this directive when appropriate.

2. Ensuring that privacy requirements are incorporated, as appropriate, into procurement requests/agreements and statements of work for information technology contracts and agreements.

3. Ensuring that solicitation documents/agreements (such as requests for proposals or requests for applications) for information systems and services include, either explicitly or by reference, applicable security, and privacy requirements, including security and privacy controls as specified in the Information Security Program plan, System Security Plan, or in applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance.

4. Ensuring that requirements, in solicitation documents/agreements for information systems and services, permit updating privacy controls as new threats/vulnerabilities are identified and as new technologies are implemented.

6685.04r - Contracting Officer/Contracting Officer Representative/Sponsors

The Contracting Officer, Contracting Officer Representatives, and Forest Service sponsors are responsible for:

1. Reviewing requirements to determine whether the contract will involve the handling of sensitive PII or design, development, or operation of a system of records on individuals to accomplish a Forest Service function.

2. Ensuring the availability, in accordance with Forest Service procedures, applicable Forest Service privacy directives.

3. Ensuring the contract work statement specifically identifies the system of records on individuals and the design, development, or operation work to be performed.

4. Ensuring the availability, in accordance with Forest Service procedures, agency rules and regulation implementing the Privacy Act.

5. Ensuring all contracts contain records management provisions set forth in FSM 6230.3, item 19 (or its successor).

6685.04s - Grants Management Specialists/Sponsors

The Grants Management Specialists and Forest Service sponsors are responsible for:

1. Reviewing requirements to determine whether the agreement will involve the handling of sensitive PII or design, development, or operation of a system of records on individuals to accomplish a Forest Service function.

2. Ensuring the availability, in accordance with Forest Service procedures, applicable Forest Service privacy directives.

3. Ensuring the agreement work statement specifically identifies the system of records on individuals and the design, development, or operation work to be performed.

4. Ensuring the availability, in accordance with Forest Service procedures, agency rules and regulation implementing the Privacy Act.

5. Ensuring all agreements contain records management provisions set forth in FSM 6230.3, item 19 (or its successor).

6685.04t - Information System Users

Information System Users are responsible for:

1. Adhering to the Forest Service requirements regarding the use of Forest Service IT resources, data, and information systems specific rules of behavior for information systems to which they have been granted access.

2. Adhering to Forest Service security and privacy policies as well as related Federal policy contained in the Privacy Act, FOIA, and Forest Service IT policies.

3. Reporting any incident where PII or other sensitive Agency data may have been lost, stolen, or compromised in accordance with USDA guidelines.

4. Not disclosing any personal information contained in any system of records except as authorized.

5. Protecting and properly disposing of any and all media, including portable and removable devices, that may contain sensitive information and according to USDA Guidelines, reporting any incident where media protection requirements may have been compromised to their Supervisor and to the USDA Cyber Incident Response and Recovery Branch (CIRRB) at *cyber.incidents@usda.gov*. Protection should include the use of appropriate encryption of the devices, storage of PII in Forest Service approved locations, such as Pinyon/Box to ensure encryption while the data is at rest and implementing encryption when transmitting files that may leave the USDA network.

6. Confirming the accuracy, relevance, timeliness, and completeness of information during the collection or creation of PII.

7. Collecting PII directly from the individual to the greatest extent practicable.

8. Checking for, and correcting as necessary, any inaccurate or outdated PII used by programs or systems. Revalidate that PII collected is still accurate.

9. Minimize the use of PII for testing, training, and research. Implement controls to protect PII when used for testing, training, and research and where feasible, use techniques to minimize the risk.

10. Minimize the creation of documents, spreadsheets, databases or lists that contain PII where possible and refrain from using Social Security Numbers unless absolutely necessary in those documents/spreadsheets/databases/lists.

11. Refrain from using forms or other methods to collect information including PII from the public unless the information collection has received approval from OMB.

6685.05 - Definitions [Reserved]

6685.06 - References [Reserved]

6685.1 - Protecting the Confidentiality of Personally Identifiable Information

1. Design information systems to support privacy by employing technologies and system capabilities that automate privacy controls on the collection, use, and disclosure of PII.

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

3. Collect and retain PII in accordance with Federal law and FSM 1380.3.

4. Develop, disseminate, and update reports to USDA, and other oversight bodies, as appropriate to demonstrate accountability with specific statutory and regulatory privacy program mandates, and to senior management and other personnel with responsibility for monitoring privacy program progress and compliance.

5. Keep an accurate accounting of disclosures of information held in each system of records under Forest Service control and retain the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer (see FSH 6209.11, Ch. 40, file code 6270 for additional information on records retention). Each accounting of disclosure must:

    a. Contain the date, nature, and purpose of each disclosure of a record and the name and address of the person or agency to which the disclosure was made.

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

6685.2 - Privacy Threshold Analysis, Privacy Impact Assessment and System of Records Notice

1. Document and implement a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

2. Conduct a PTA for all information systems, programs, or other activities to determine potential for privacy risk.

3. Conduct PIAs for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures.

4. Conduct a PTA and a PIA if needed:

    a. Before the acquisition and/or development of any new system that will process PII. [RA-8 PRIV]

    b. Where a system change may create new privacy risks.

    c. To evaluate the system before initiating a new electronic collection of information. [RA-8 PRIV]

    d. Annually, in accordance with continuous monitoring guidance.

5. Each PIA must include, at a minimum, the information required to conform to Office of Management and Budget Memorandum 03-22, USDA Departmental Regulations, and Forest Service procedures.

6. Include Privacy Act Statements on forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected. [PT-5(2) PRIV]

7. Include Federal Register Notice and OMB control numbers in accordance with the guidance provided in the Paperwork Reduction Act when collecting information from 10 or more members of the public in a 12-month period.

8. Maintain System(s) of Record Notification (SORNs) when a system of record is required, and ensure the information is retrieved by name or other unique identifier. [PT-6(a) PRIV]

    a. Document legal authority, collection, use, maintenance, and sharing of PII in SORNs.

    b. Provide individuals the ability to access their PII maintained in SORNs.

    c. Publish PII access procedures in SORNs.

    d. Publish SORNs in the Federal Register and USDA approved website, subject to required oversight processes, for systems containing PII. [PT-6(b)PRIV]

    e. Keep SORNs accurate, up-to-date, and scoped in accordance with policy. [PT-6(d) PRIV]

    f. Review all routine uses published in the SORNs, to ensure continued accuracy and that routine uses continue to be compatible with the purpose for which the information was collected. [PT-6(1) PRIV]

    g. Review all Privacy Act exemptions claimed for the system of records, to ensure they remain appropriate and necessary in accordance with privacy laws, that they have been promulgated as regulations, and that they are accurately described in the SORN. [PT-6(2) PRIV]

9. Document the results in Cyber Security Assessment and Management (CSAM), the USDA's official Federal Information Security Management Act reporting tool.

6685.3 - Use of Privacy Information

1. Determine and document the legal authority that permits the collection, use, maintenance, and sharing of PII. Describe the purpose(s) for which PII is collected, used, maintained, and shared in privacy notices. [PT-2(a) PRIV, PT-3(a, b) PRIV]

2. Use PII internally only for the authorized purpose(s) identified in the Privacy Act and/or in public notices. [PT-2(b) PRIV]

3. Share PII externally, only for the authorized purposes identified in the Privacy Act and/or described in the notice(s) or for a purpose that is compatible with those purposes.

4. Enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, where appropriate, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used.

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

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

7. Monitor changes in processing PII and implement reviews to ensure that changes are made in accordance with current OMB, USDA, and Forest Service guidance. [PT-3(d) PRIV]

6685.4 - Data Management

6685.4a - Data Quality/Data Integrity

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

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

3. Check for, and correct as necessary, any inaccurate or outdated PII used by programs or systems. Issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. [SI-18 PRIV]

4. Request that the individual or individual's authorized representative revalidate that PII collected is still accurate.

5. Correct or delete personally identifiable information upon request by individuals or their designated representatives. [SI-18(4) PRIV]

6. Document processes to ensure the integrity of PII through existing security controls.

7. Work with USDA Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements and to ensure that those agreements comply with the computer matching provisions of the Privacy Act.

8. Publish Computer Matching Agreements on a USDA approved public website.

9. When a system or organization processes information for the purpose of conducting a matching program: [PT-8 PRIV]

    a. Obtain approval from the USDA Data Integrity Board to conduct the matching program.

    b. Develop and enter into a computer matching agreement.

    c. Publish a matching notice in the Federal Register.

    d. Verify independently the information produced by the matching program before taking any required adverse action against an individual, and

    e. Provide individuals with notice and an opportunity to contest the findings before taking adverse action against an individual.

6685.4b - Minimization of Personally Identifiable Information

1. Identify the minimum PII elements that are relevant and necessary to accomplish the legally authorized purpose of collection.

2. Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent. [PT-3(c) PRIV]

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

4. Locate and remove/redact specified PII and/or use anonymization and de-identification techniques where feasible and within the limits of technology to permit use of the retained information while reducing sensitivity and reducing the

risk resulting from disclosure. Eliminate the use of SSN where possible or obtain the appropriate waivers if SSN use is required.

5. Implement controls to protect PII when used for testing, training, and research. Where feasible, use techniques to minimize the use of and risk to privacy information during testing, training, or research activities. [SI-12(2) PRIV]

6685.4c - Data Retention and Disposal

1. Retain each collection of PII to fulfill the purpose(s) identified in the notice or as required by law.

2. Dispose of, destroy, erase, and/or anonymize the PII, regardless of the method of storage, in accordance with a National Archives and Records Association-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access (see FSM 6209.11, Ch. 30 and 40 for additional details).

3. Use Forest Service approved techniques or methods to ensure secure deletion or destruction of PII including originals, copies, and archived records. [SI-12(3) PRIV]

4. Configure information systems, where feasible, to record the date PII is collected, created, updated, deleted, or archived under an approved record retention schedule. Contact the Forest Service Records Officer for information on applicable records retention schedules for information systems.

5. Remove PII from datasets (de-identification) when such information is no longer necessary to satisfy the requirements envisioned for the data. [SI-19(a) PRIV]

6. Review and evaluate the effectiveness of de-dentification processes. [SI-19(b) PRIV]

6685.4d - Individual Consent, Access

1. Provide processes, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of PII prior to collection. [PT-4 PRIV]

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

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

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

5. Implement mechanisms to support itemized or tiered consent for specific uses of PII data.

6. Provide individuals the ability to have access to their PII maintained in the system(s) of records.

7. Publish access procedures in SORNs.

Note: Reference FSM 6240 for rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records, Privacy Act appeals, complaints, and requirements and OMB policies and guidance on the proper processing of Privacy Act requests.

6685.4e - Dissemination and Inventory of Privacy Program Information

1. Provide a process for individuals to have inaccurate PII maintained by the organization corrected or amended, as appropriate.

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

3. Implement a process for receiving and responding to complaints, concerns, or questions from individuals about the Forest Service privacy practices.

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

5. Provide each update of the PII inventory to the CIO or Information Security Official to support the establishment of information security requirements for all new or modified information systems containing PII.

6. Ensure that the public has access to information about privacy activities and is able to communicate with the Senior Agency Official for Privacy/Chief Privacy Officer.

7. Ensure that privacy practices are publicly available through Forest Service approved websites or otherwise.

6685.4f - Transparency

1. Provide effective notice to the public and to individuals regarding: [PT-5]

    a. Activities that impact privacy, including collection, use, sharing, safeguarding, maintenance, and disposal of PII.

b. Authority for collecting PII.

c. The choices, if any, individuals may have regarding how PII is used and the consequences of exercising or not exercising those choices.

d. The ability to access and have PII amended or corrected if necessary.

2. The notice provided to individuals about processing PII must: [PT-5 PRIV]

   a. Be available to individuals

   b. Be clear and easy-to-understand, expressing information about PII processing in plain language.

   c. Identify the authority that requires the processing of PII.

   d. Identify the purpose(s) for processing PII.

3. Describe:

   a. The PII collected and the purpose(s) for which it is collected.

   b. How PII is used internally.

   c. How PII is shared with external entities, the categories of those entities, and the purposes for such sharing.

   d. Whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent.

   e. How individuals may obtain access to PII.

   f. How the PII will be protected.

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

5. Provide real-time and/or layered notice when PII is collected.

6685.4g - Specific Categories of Personally Identifiable Information

1. Apply USDA or SAOP-identified processes for specific categories of PII. [PT-7 PRIV]

2. For systems that process Social Security numbers: [PT-7(2) PRIV]

a. Eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives for personal identifiers;

b. Do not deny any individual any right, benefit, or privilege provided by law because of an individual's refusal to disclose their Social Security number; and

c. Inform all individuals, who are requested to disclose Social Security numbers, that the disclosure is mandatory or voluntary, the statutory or the authority used for the request, and its intended use.

3. Prohibit the processing of information describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute, by the individual, or if pertinent to and within the scope of an authorized law enforcement activity. [PT-7(2) PRIV]

6685.5 - Additional Privacy Controls for High Value Asset Systems

Note: These policies only apply to information systems designated by USDA as a High Value Asset System.

6685.5a - Personally Identifiable Information Processing Purposes

1. Attach data tags supporting the tracking of Forest Service-designated processing purposes to designated elements of PII. [PT-3(1) PRIV]

2. Track processing purposes of PII using Forest Service-approved automated mechanisms. [PT-3(2) PRIV]