U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	NUMBER: DR 3575-004
SUBJECT: Information Technology Security Baselines and Security Control Tailoring	DATE: November 21, 2023
OPI: Office of the Chief Information Officer, Cybersecurity & Privacy Operations Center	EXPIRATION DATE: November 21, 2028

Section Page

1. PURPOSE

a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) *Information Technology (IT) Security Controls Baselines* for information systems.

b. The USDA derives IT security baselines (ITSB) from the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53B, *Control Baselines for Information Systems and Organizations*, listing of controls and control enhancements assigned to NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, security control families.

c. This DR guides USDA Mission Areas, agencies, and staff offices to develop, implement, maintain, and document ITSB. This DR also instructs on tailoring security and privacy controls to protect USDA information systems against risks.

2. SCOPE

a. This DR applies to all:

(1) USDA Mission Areas, agencies, staff offices, and personnel who work for or on behalf of USDA. The term "USDA personnel" encompasses USDA employees, appointees, contractors, partners, interns, fellows, affiliates, and volunteers;

(2) Federal information, per DR 3080-001, *Records Management*, in any medium or form generated, collected, provided, transmitted, stored, maintained, or accessed by or on behalf of USDA; and

(3) Information systems or services (including cloud-based services) used or operated by USDA, contractors, or other organizations on behalf of or funded by USDA, and interconnections between or among systems or services.

b. Nothing in this policy alters the requirements for protecting national security systems or information. This includes those identified in the *Federal Information Security Modernization Act of 2014* (FISMA) and the Committee on National Security Systems (CNSS) policies, directives, instructions, and standards, and Intelligence Community policies, directives, and instructions.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This DR supersedes DR 3140-001, *USDA Information Systems Security Policy*, dated May 15, 1996.

b. This DR is effective immediately when published and will remain in effect until it is superseded, or it expires.

c. This DR addresses and meets the requirements of:

(1) FISMA, 44 United States Code (U.S.C.) §§ 3551, *et seq*.;

(2) *Chief Information Officer*, 7 Code of Federal Regulations (CFR) § 2.32;

(3) *Federal Agency Responsibilities*, 44 U.S.C. § 3506(b)(2);

(4) *Privacy Act of 1974* (*Privacy Act*), 5 U.S.C. § 552a;

(5) Office of Management and Budget (OMB), Circular A-130, *Managing Information as a Strategic Resource*;

(6) NIST, SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*;

(7) NIST, SP 800-53B, *Control Baselines for Information Systems and Organizations*;

(8) NIST, SP 800-37, Revision 2, *Risk Management Framework (RMF) for Information Systems and Organizations*;

(9) NIST, SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*; and

(10) USDA, DR 3180-001, *Information Technology Standards*.

d. All USDA Mission Areas, agencies, and staff offices will align their ITSB and security and privacy control tailoring policies with this DR within 6 months of the publication date.

e. All Mission Areas, agencies, and staff offices will implement ITSB, and update respective system security plans (SSP) as needed for all information systems.

f. All new information system authorizations (e.g., authorization to operate (ATO)) must be assessed and issued under minimum ITSB.

4. BACKGROUND

a. This policy follows NIST SP 800-53B. The requirements for security and privacy controls derive from applicable laws, Executive Orders (E.O.), directives, regulations, policies, standards, and mission needs.

b. Security controls are policies, procedures, and technical configurations which an organization implements on their information systems to protect the confidentiality, integrity, and availability of information.

c. Privacy controls ensure compliance with relevant privacy requirements, and manage privacy risks.

d. Control baselines are a collection of controls assembled to address the protection needs of a group, organization, or community of interest.

e. The selection, design, and effective implementation of controls are important tasks that can impact an organization's assets and operations, and the welfare of individuals and the Nation.

f. NIST SP 800-37, Revision 2, defines two approaches for the selection of security and privacy controls: a baseline control selection, and a tailored control selection. Tailored controls may also be called overlays.

g. Overlays complement the NIST control baselines by providing an opportunity to add or eliminate controls to accommodate organizational requirements, while continuing to protect information proportionate to risk.

h. Organizations can use overlays to customize control baselines by describing control applicability and providing interpretations for specific technologies.

5. POLICY

a. This USDA ITSB policy will assist system owners in establishing ITSB and creating tailored security and privacy control baselines for their specific information systems.

b. System owners must align risk management practices defined in NIST SP 800-37, Revision 2 to effectively manage their security and privacy risks. ITSB and overlays aid system owners to select the baseline controls for their specific information system logical boundary through the following:

(1) Categorize the information system boundary, and document the system description using the following:

(a) System design with required documentation;

(b) Systems supporting RMF roles;

(c) Boundary authorization information;

(d) Document the type of information, typical usage (e.g., stored, accessed, or processed), and the potential impact should a compromise of confidentiality, integrity, or availability occur. Base this security categorization on the high watermark of information type impact levels. Use Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems* for security categorization for guidance; and

(e) Review and document information stored, accessed, processed, or exchanged from USDA or relative external information system for identification of other possible sensitive information with the potential of raising the high watermark of the information system boundary.

(2) Select the baseline system security and privacy controls through the following:

(a) Document the baseline controls applicable to NIST SP 800-53, Revision 5;

(b) Determine if there are privacy risks arising from processing personally identifiable information (PII). If there are risks, then system owners must create a privacy control baseline in addition to security baseline controls. NIST SP 800-53B explains the privacy controls in further detail. The USDA Chief Information Officer (CIO), serving as the Senior Agency Official for Privacy (SAOP) oversees the management of privacy controls; and

(c) Follow NIST SP 800-53, Revision 5 security controls for low, moderate, or high.

(3) System owners will review and follow control baseline assumptions through the following:

(a) Ensure the information in organizational systems is persistent (e.g., days, weeks);

(b) Determine if information systems are multi-user (either serially or concurrently) in operation;

(c) Determine if information (e.g., controlled unclassified information (CUI)) requires additional access controls;

(d) Determine if the information system resides in a networked environment, and is general purpose in nature;

(e) Determine if USDA has provided the necessary structure, resources, and infrastructure to implement the controls; and

(f) Determine if any of the above assumptions are not valid, then some of the security controls allocated to the control baseline may not apply.

(4) System owners must tailor the security and privacy control baselines to align with the unique and specific circumstances of their information system boundary. They must label each control and control enhancement through the following:

(a) Document inherited common controls from the most recent SSP (within 12 months);

(b) Document system-specific or hybrid security controls, per the most recent security assessment, and continuously monitored; and

(c) Document known acceptance of risk:

1 The system's Authorizing Official (AO) has lone authority to accept risks for required ITSB controls and policies, except for those explicitly requiring acceptance by the USDA CIO;

2 Risk-based acceptance requests must document the following information:

a A justification statement explaining the disregard of the control;

b A statement explaining and describing which compensating controls they will use to reduce associated risks;

c A risk statement describing all residual or new risk resulting from this decision; and

d A plan of action and milestones (POA&M) for relevant unimplemented controls.

3 Render a risk decision where policy requires AO approval of risk, the rendered decision; and

4 Reference all risk-based acceptances in the relevant system security documentation (e.g., SSP, Risk Assessment) and made available to the USDA Chief Information Security Officer (CISO) upon request.

(5) When controls in the initial baselines do not apply to every component in the system, system owners must work with the AO to make risk-based decisions on where to apply or allocate specific security controls to satisfy security and privacy requirements.

(6) System owners will follow scoping considerations when tailoring the security and privacy control baselines through the following:

(a) Use overlays, which are the foundation for determining the needed set of system controls;

(b) Tailor the baseline if operational and environmental factors diverge significantly from baseline assumptions, (i.e., a FISMA boundary is an application only hosted in the cloud), consider the following common environmental factors:

1 Mobile devices;

2 Single-user systems;

3 Bandwidth limitations;

4 Air-gapped systems;

5 Internet of Things devices;

6 Limited functionality systems (i.e., printers, digital cameras);

7 Systems processing, storing, or transmitting non-persistent information;

8 Application-only systems; and

9 Systems requiring public access.

(c) Controls supporting only one or two of the security objectives may be downgraded to the corresponding control in a lower baseline. Modification or elimination of controls may be required if not defined in a lower baseline. Downgrading a control must first reflect the FIPS PUB 199 security category for the supported security objectives. Then the downgrade must consider FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, impact level (i.e., high watermark). Downgrades must have an organizational risk assessment, and cannot adversely affect the level of protection for the security-relevant information within the system;

(d) USDA does not allow use of controls whose implementation has the potential to degrade, debilitate, or interfere with USDA's overall mission and business functions. Decisions on the propriety of control implementation must always include legislative, regulatory, and policy requirements;

(7) System owners will not tailor controls to meet legislative, regulatory, or policy requirements without the approval of the AO; and

(8) Tailoring will not arbitrarily remove security and privacy controls from baselines. Tailoring decisions will be defensible based on mission and business needs, a sound rationale, and explicit risk-based determinations;

c. Designated controls (i.e., common, hybrid, or system-specific) allocated to the individual system elements (e.g., machine, physical, or human elements) must meet security and privacy requirements. These controls must also:

(1) Identify and implement compensating controls, approved by the AO, for any incompatible controls on the information system; and

(2) Utilize risk assessment results to determine the sufficiency of controls in the tailored baseline. The respective AO and Information System Security Manager (ISSM) must review and approve the determination.

d. When instituting control tailoring, the system owners and the AO must work with their ISSM to provide complete implementation details for all controls employed on the system. They must also detail this information in the system's SSP, without exceptions.

e. System owners may tailor out controls with this guidance. When choosing not to employ a control, the respective SSP documentation must contain all the following information without exception:

(1) A justification statement explaining the disregard of the control. Two acceptable reasons are the scoping guidance in NIST SP 800-53, Revision 5 prevents employment, and control implementation resulting in technical or operational incompatibility on a specific system;

(2) A statement describing which compensating controls they will use to offset associated risks;

(3) A risk assessment describing all residual or new risks resulting from this decision; and

(4) A POA&M for relevant, unimplemented controls.

f. System owners must meet all USDA compliance requirements including those established in this DR. The Office of the Chief Information Officer (OCIO) Cybersecurity & Privacy Operations Center (CPOC) will ensure compliance by auditing and reviewing security and privacy control assessments of a sampling of systems based on this ITSB. These assessments will include a review of the controls baseline for a given system based on the system's FIPS PUB 199 impact level. System owners will categorize the status of each control in the applicable baseline as:

(1) Implemented and functioning effectively to provide a minimum level of security;

(2) Implemented but not functioning effectively, with either a subsequent POA&M detailing steps to facilitate effective functioning, or the AO’s documented risk acceptance;

(3) Not implemented, with supporting documentation as required; or

(4) Other, with detailed explanation.

g. USDA Mission Areas, agencies, and staff offices will document and analyze lessons learned on their programs, control activities, procedures, and tasks. They will use this qualitative and quantitative data to assess effectiveness and to guide process improvement.

6. ROLES AND RESPONSIBILITIES

a. The USDA CIO, or delegated staff, will:

(1) Serve as the final approving authority Departmentwide for IT requirements and standards adoption;

(2) Serve as the final approving authority for Mission Areas, agencies, or staff offices requesting policy waivers and workstation requirement exceptions;

(3) Serve as the SAOP, and will:

(a) Develop, implement, and maintain a Departmental privacy program. The program will ensure programs and systems handle PII from creation to disposal in compliance with all applicable statues, regulations, and policies;

(b) Ensure the Department's implementation of information privacy protections;

(c) Ensure the availability of sample cascading goals and objectives for inclusion in performance plans of employees with privacy responsibilities;

(d) Convene the USDA Data Integrity Board (DIB) to fulfill computer matching responsibilities per DR 3450-001, *Computer Matching Program Involving Personally Identifiable Information*;

(e) Approve the establishment or amendment of *Privacy Act* documentation for publication in the *Federal Register*;

(f) Ensure that appropriate changes to privacy policies, procedures, standards, and guidelines occur in a timely manner;

(g) Develop and maintain the USDA Privacy Program Plan, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks;

(h) Develop and maintain a privacy continuous monitoring strategy and program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and to manage privacy risks;

(i) Conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the Department and across all risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks;

(j) Identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;

(k) Designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the Department;

(l) Review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;

(m) Review and approve the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;

(n) Review and approve the privacy plans for Departmental, Mission Area, agency, and staff office information systems prior to authorization, reauthorization, or ongoing authorization;

(o) Review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to AOs making risk determination and acceptance decisions;

(p) Ensure the appropriate training and education regarding privacy laws, regulations, policies, and procedures concerning the handling of PII are afforded to USDA personnel;

(q) Facilitate and negotiate agreements with senior management and establishing relationships with partners in private industry and other Federal agencies to foster the development and sharing of privacy-related best practices; and partnering with the OCIO to ensure all aspects of the USDA Privacy Program are incorporated into the Department's enterprise infrastructure, IT, and IT security programs; and

(r) Coordinate with the CISO, OCIO Service Center Associate CIOs, (ACIO) and other Departmental, Mission Area, agency, and staff office officials in implementation of these requirements;

(4) Sponsor and articulate risk management perspectives on behalf of their role and Departmental perspective; and

(5) Serve as the Senior Agency Official for CUI per DR 3440-003, *Controlled Unclassified Information (CUI) Program*, Section 6c.

b. The Director of the Office of Budget and Program Analysis, serving as the Chief Risk Officer and Senior Agency Official for Risk Management will:

(1) Establish and oversee a process for managing enterprise risks;

(2) Establish and review Departmentwide risk management roles and responsibilities;

(3) Manage and oversee organizational risk assessments to ensure consistent and effective risk-based decisions;

(4) Establish Departmentwide forums to consider all types and sources of risk (including aggregated risk); and

(5) Ensure consistent messaging, processing, and communication of decisions and actions within the purview of the Senior Agency Official for Risk Management.

c. The USDA CISO will:

(1) Ensure the development and maintenance of ITSB in accordance with this DR;

(2) Oversee the Department, Mission Areas, agencies, and staff offices compliance with this directive;

(3) Ensure Mission Area Assistant CISOs (ACISO) and ISSMs receive updated ITSB requirements and guidance;

(4) Advise the CIO of IT security advances that can be used Departmentwide, and provide reduced costs for IT security efforts;

(5) Advise the CIO of supply chain risks for individual information systems;

(6) Advise system owners on appropriate implementation of ITSB to ensure information systems maintain an operational security posture;

(7) Report to the CIO and external entities (e.g., OMB, Government Accountability Office, and Congress) on USDA's IT security program status;

(8) Coordinate with the USDA CIO, Mission Area Assistant CIOs, and ACISOs to deliver and operate centrally managed, Departmentwide, common cybersecurity technical controls;

(9) Deliver comprehensive cybersecurity leadership in developing and implementing an enterprisewide, trusted environment in support of all USDA components;

(10) Provide enterprise security capabilities;

(11) Provide technical guidance, engineering, and operational services;

(12) Deliver a centralized threat awareness and security analytics capability;

(13) Deliver a framework for tracking, reporting, and prompt incident response;

(14) Complete security, assessment and authorization via the USDA RMF process for all USDA systems;

(15) Oversee cybersecurity incident management in accordance with DR 3505-005, *Cybersecurity Incident Management*; and

(16) Manage the USDA high value assets (HVA) program.

d. The USDA Chief Privacy Officer will:

(1) Advise the SAOP on privacy matters;

(2) Develop and oversee implementation of Departmentwide policies and procedures relating to the *Privacy Act* and manage PII contained in *Privacy Act* systems of record in compliance with its provisions;

(3) Advocate strategies for data and information collection and dissemination to ensure Departmental privacy policies and principles are reflected in all operations;

(4) Ensure Departmental information protection policies and procedures comply with statutory and Government policy requirements;

(5) Verify Mission Area, agency, and staff office adherence to relevant information protection policies and procedures;

(6) Provide expertise in the selection of Privacy security control overlays, in accordance with FISMA, the *Privacy Act*, and OMB A-130; and

(7) Assign a Department-defined assessment timeline to each control. Timelines must fulfill requirements for privacy risk management.

e. The USDA Privacy Architect within OCIO, CPOC will:

(1) Address system privacy requirements necessary to protect individual's privacy in all aspects of enterprise architecture; and

(2) Coordinate with the Chief Enterprise Architect to determine the optimal placement of systems or system elements within the enterprise architecture to address security and privacy issues.

f. The USDA Chief Data Officer will:

(1) Protect USDA information and retain that responsibility when the information is shared with other organizations;

(2) Provide input to system owners regarding:

(a) Types of information and associated risks;

(b) Security requirements and controls necessary for protecting information where it is processed, stored, or transmitted;

(c) Determinations of categorization, storage, protection, and access and privilege; and

(d) Risk-related situations involving their data, and risk exposure approval.

g. The USDA CUI Program Manager within the OCIO Information Resource Management Center (IRMC) will report to the USDA CIO, serving as the Senior Agency Official for CUI regarding program management functions, as specified in DR 3440-003.

h. OCIO Service Center ACIOs will:

(1) Serve as the AO for their OCIO service center (e.g., CPOC, Digital Infrastructure Services Center, or IRMC) FISMA information system boundaries;

(2) Appoint their Authorizing Official Designated Representative (AODR);

(3) Develop policies, regulations, and compliance requirements for the IT environment. Provide channels for Mission Area, agency, and staff office input and approval of those policies, regulations, and compliance requirements;

(4) Provide management and oversight activities related to business, performance, application, data, infrastructure, and security configurations;

(5) Review and monitor compliance with established policy requirements and standards without impairing business functions or mission requirements; and

(6) Report compliance and deviations to OMB.

i. Mission Area Assistant CIOs will:

(1) Serve as the AO for their Mission Area FISMA information system boundaries;

(2) Implement and maintain business, performance, application, data, infrastructure, and security configuration settings:

(a) Document all standard configuration deviations, providing a detailed rationale in a waiver request to the USDA CISO;

(b) Request waivers substantiating all policy exception requirements from the USDA CISO;

(c) Provide corrective action plans to the USDA CISO for issues not authorized as an approved deviation; and

(d) Ensure adherence to and compliance with NIST and FIPS PUB standards prior to utilizing International Organization for Standardization standards.

(3) Appoint their AODR; and

(4) Implement policies, requirements, and standards for the IT environment, and:

(a) Develop new, and review existing, internal procedures and controls in support of this policy; and

(b) Establish communication between system owners and an identified point of contact in OCIO.

j. AOs will:

(1) Appoint their AODR;

(2) Grant or deny ATO in alignment with NIST SP 800-37, Revision 2;

(3) Accept residual risk(s) for enterprise systems and networks. The AO cannot delegate or share this duty to the AODR or another individual;

(4) Oversee the budget and business operations of their respective information systems within the USDA;

(5) Approve system security requirements, SSP, interconnection security agreements, and Memoranda of Agreement or Memoranda of Understanding, and POA&Ms. Determine whether significant changes in the information systems or operational environments require reauthorization; and

(6) Coordinate their activities with the USDA CIO, USDA CISO, Common Control Providers (CCP), system owners, their Information System Security Officer (ISSO), Security Control Assessor (SCA), and other interested parties during the security authorization process.

k. AODRs will act on behalf of an AO to coordinate and conduct the required activities associated with the security authorization process.

l. Mission Area ACISOs will:

(1) Collaborate with the USDA CISO through their Mission Area Assistant CIO on risk management related issues or situations for their Mission Area;

(2) Ensure the development and maintenance of the Mission Area's disaster recovery plan;

(3) Conduct annual continuous monitoring of the Mission Area's IT security program to ensure compliance with established policies and procedures;

(4) Implement IT and cyber workforce planning;

(5) Provide overall management, leadership, and direction to the IT security program;

(6) Develop, maintain, and oversee the Mission Area IT security policy;

(7) Ensure IT security program implementation complies with FISMA; and

(8) Address IT security requirements and resource needs through IT investment and capital programming processes.

m. SCAs will:

(1) Provide guidance to their component offices for performing security control assessments;

(2) Ensure personnel review the SSP prior to initiating the security control assessment. Ensure the SSP contains a set of security controls meeting the stated security requirements;

(3) Ensure a thorough assessment of the managing, operational, technical, and enhanced security controls employed within or inherited by an information system. The assessment's goal is to determine overall control effectiveness;

(4) Document weaknesses and deficiencies discovered in system and environmental assessments;

(5) Recommend corrective actions to mitigate identified vulnerabilities; and

(6) Review the final security assessment report (SAR).

n. The Director of the OCIO, CPOC, Security Management Division (SMD) will ensure a sampling security and privacy control assessments are audited and reviewed for alignment with the USDA ITSB.

o. The USDA HVA Program Manager within OCIO, CPOC, SMD will:

(1) Incorporate emerging Federal laws, regulations, and other authoritative guidance for the protection of HVA;

(2) Account for emerging threats and technologies; and

(3) Provide expertise in the selection and application of HVA security control overlays, in keeping with the Assessment Evaluation and Standardization Program from the Department of Homeland Security, Cybersecurity Infrastructure and Security Agency.

p. Mission Area, Agency, and Staff Office ISSMs will:

(1) Serve as a consultant to their Mission Area Assistant CIO and senior management;

(2) Collaborate with their ISSO to maintain an appropriate operational security posture for an information system or program;

(3) Manage the information system security efforts for their entire Mission Area, agency, or staff office;

(4) Plan, budget, review, and consolidate their Mission Area, agency, or staff office security reports;

(5) Function as consultants for their ISSO, working with them to resolve highly technical matters when necessary;

(6) Manage the Mission Area, agency, or staff office Information System Security Program;

(7) Support the strategic security program requirements;

(8) Consolidate individual reports from all functional and operational units into one Mission Area, agency, or staff office combined report (i.e., monthly scans, patches, incidents) for higher level management;

(9) Monitor the progress of their Mission Area, agency, or staff office ISSO to ensure they meet the necessary program security requirements;

(10) Coordinate Mission Area, agency, and staff office incident response with their Mission Area, agency, or staff office ISSO to include all associated actions necessary to mitigate the risk to information systems;

(11) Oversee the implementation of Mission Area, agency, and staff office security policies, procedures, and guidelines;

(12) Ensure proper assessments, reviews and updates of all security and privacy controls;

(13) Ensure the security controls to external information systems maintain an acceptable level of risk to information and information systems;

(14) Ensure control documentation and submission of requirements to the USDA CISO for inclusion in Departmentwide compliance reporting, as needed;

(15) Ensure control standards including methods, technology, devices, configurations, and tools balance risk and business needs;

(16) Advise system owners about the secure implementation of technologies;

(17) Ensure privileged users cannot make unauthorized changes to audit settings; and

(18) Disseminate USDA security policy and procedures.

q. Mission Area, Agency, and Staff Office ISSOs will:

(1) Maintain an appropriate operational security posture for an information system or program in direct collaboration with system owners;

(2) Provide day-to-day security administration for information systems;

(3) Develop and maintain the system security authorization , and implement and monitor the system security controls;

(4) Serve as the principal advisor to their Mission Area Assistant CIO and ACISO, and to system owners on all security matters for the information system;

(5) Maintain an active role in developing and updating the SSP as well as in managing and controlling changes to the system and assessing the security impact of those changes;

(6) Assist their ISSM with the security assessment and authorization process;

(7) Serve as key advisor in risk assessments of all systems and mitigating vulnerabilities;

(8) Assist system owners and ISSM in the development, testing, and maintenance of system contingency plans, back-up, and storage procedures and

(9) Audit and monitor applications, system and security logs for security threats, vulnerabilities, and suspicious activities, reporting suspicious activities to their Mission Area, agency, or staff office ISSM.

r. Mission Area, Agency, and Staff Office Privacy Officers will ensure their systems comply with privacy requirements.

s. The Chief Enterprise Architect within the OCIO IRMC, Enterprise Architecture Division will:

(1) Build a holistic view of the mission and business functions, processes, information, and IT assets;

(2) Implement an enterprise architecture strategy that facilitates effective security and privacy solutions;

(3) Coordinate with the Chief Privacy Officer and the Privacy Architect to determine the optimal placement of systems or system elements within the enterprise architecture and to address security and privacy issues between systems and the enterprise architecture;

(4) Assist in reducing complexity within the IT infrastructure to facilitate security;

(5) Assist with determining appropriate control implementations and initial configuration baselines as they relate to the enterprise architecture;

(6) Collaborate with system owners and AOs to facilitate authorization boundary determinations and allocation of controls to system elements;

(7) Sponsor and articulate risk management perspectives on behalf of their role and Departmental perspective;

(8) Assist with integration of the organizational risk management strategy and system-level security and privacy requirements into program, planning, and budgeting activities, the system development lifecycle, acquisition processes, security, privacy and systems engineering processes;

(9) Address information security requirements necessary to protect the organization's core missions and business processes in all aspects of enterprise architecture;

(10) Communicate with the Information System Security Engineers, and coordinate with the system owners, CCPs, and ISSOs on the allocation of security controls as system specific, hybrid, or common controls; and

(11) Advise the AO, CIO, OCIO Service Center ACIOs, and Mission Area Assistant CIOs, in collaboration with ISSO, on a range of security-related issues, and:

(a) Establish information system boundaries;

(b) Assess the severity of weaknesses and deficiencies in the information system;

(c) Manage POA&Ms;

(d) Implement risk mitigation approaches; and

(e) Manage vulnerabilities.

t. Mission Area, Agency, and Staff Office Information System Security Engineers will:

(1) Coordinate their security-related activities with USDA CISO, their Mission Area ACISO, system owners, CCPs, and ISSOs;

(2) Serve as an integral part of the development team (e.g., integrated project team) designing and developing organizational information systems or upgrading legacy systems; and

(3) Employ best practices when implementing security controls within an information system including software engineering methodologies, system and security engineering principles, secure design, secure architecture, and secure coding techniques.

u. OCIO Service Center CCPs will:

(1) Develop, implement, assess, operate, and monitor common controls (i.e., security and privacy controls inherited by information systems);

(2) Function as system owners when common controls reside within the respective information system;

(3) Document the organization-identified common controls in an SSP (or equivalent document prescribed by the organization);

(4) Ensure independent assessors conduct required assessments of common controls with an appropriate level of independence defined by the organization;

(5) Document assessment findings in a SAR;

(6) Create a POA&M for all controls having weaknesses or deficiencies;

(7) Create the SSP, SAR, and POA&M for common controls for system owners inheriting those controls; and

(8) Sponsor and articulate risk management perspectives on behalf of their role and Departmental perspective.

v. System Owners will:

(1) Ensure the processes to create, maintain, revoke, and verify security and privacy controls comply with this policy;

(2) Maintain information for all applicable system accounts;

(3) Coordinate with ISSMs to decide who has access to the information system and determine the types of privileges and access rights;

(4) Ensure systems are compliant with identified control tailoring prior to production and implementation;

(5) Serve as the point of contact for the information system, responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of the information system;

(6) Develop and maintain the SSP;

(7) Ensure the system is deployed and operated according to the agreed-upon security requirements;

(8) Monitor the system and manage the hardware and software lifecycle;

(9) Manage access control;

(10) Inform key Mission Area, agency, and staff office officials of requisite information system security assessment and authorization, ensuring appropriate resources are available for the effort; and

(11) Manage risk by taking appropriate steps to reduce or remediate vulnerabilities, and provide their AO or AODR with adequate information to make risk-based decisions.

w. System Users will:

(1) Complete annual Information Security Awareness training, and other role-based training as prescribed in DR 3545-001, *Information Security Awareness (ISA) Program*;

(2) Report any known violation of IT security policies to their ISSM or immediate supervisor; and

(3) Cooperate with OCIO-CPOC and management during an investigation of suspected or confirmed security incidents (e.g., loss of PII, virus, malicious activity).

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NONCOMPLIANCE

a. DR 4070-735-001, *Employee Responsibilities and Conduct*, Section 16, *Computers and Telecommunications Equipment*, sets forth USDA developed policies, procedures, and standards on employee responsibilities and conduct regarding the use of computers and telecommunication equipment. In addition, DR 4070-735-001, Section 21, *Disciplinary or Adverse Action*, states:

(1) Any violation of the responsibilities or standards contained in this DR may be cause for disciplinary or adverse action; and

(2) Any disciplinary or adverse action taken will be consistent with the applicable laws and regulations.

b. Such disciplinary or adverse action will be consistent with applicable laws and regulations such as Office of Personnel Management regulations, OMB regulations, and the Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.

8. POLICY EXCEPTIONS

All Mission Areas, agencies, and staff offices will conform to this policy. If any Mission Area, agency, or staff office cannot meet a specific policy requirement, contact the OCIO CPOC SMD Risk Management Branch via email at POAMProgram@usda.gov to request a policy exception. Note that an approved policy exception is an acceptance of risk but does not constitute compliance.

9. INQUIRIES

Address any inquiries concerning this DR to the OCIO CPOC via email at SMD-PCB-Policy@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

ACIO	Associate Chief Information Officer (OCIO Service Center heads)
ACISO	Assistant Chief Information Security Officer
AO	Authorizing Official
AODR	Authorizing Official Designated Representative
ATO	Authorization to Operate
CCP	Common Control Provider
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CPOC	Cybersecurity & Privacy Operations Center (OCIO component)
CUI	Controlled Unclassified Information
DIB	Data Integrity Board
DM	Departmental Manual
DR	Departmental Regulation
E.O.	Executive Order
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
HVA	High Value Asset
IRMC	Information Resource Management Center (OCIO component)
ISCM	Information Security Continuous Monitoring
ISSM	Information System Security Manager
ISSO	Information System Security Officer
IT	Information Technology
ITSB	Information Technology Security Baseline
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
P.L.	Public Law
POA&M	Plan of Action and Milestones
PROM	Programmable Read-Only Memory
RMF	Risk Management Framework
ROM	Read-Only Memory
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCA	Security Control Assessor
SMD	Security Management Division (OCIO-CPOC component)

SP	Special Publication
SSP	System Security Plan
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

Access Control. The process of granting or denying specific requests for obtaining and using information and related information processing services; and to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). The process of granting or denying specific requests for obtaining and using information and related information processing services; and to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). (Source: NIST, SP 800-53, Revision 5)

Assessor. The individual, group, or organization responsible for conducting a security or privacy assessment. (Source: NIST, SP 800-37, Revision 2)

Audit. Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. (Source: NIST, SP 800-53, Revision 5)

Authorization. Access privileges granted to a user, program, or process or the act of granting those privileges. (Source: NIST, SP 800-53, Revision 5)

Authorization to Operate (ATO). The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems. (Source: NIST, SP 800-53, Revision 5)

Availability. Ensuring timely and reliable access to and use of information. (Source: NIST, SP 800-53, Revision 5)

Common Control. A security or privacy control that is inherited by multiple information systems or programs. (Source: NIST, SP 800-53, Revision 5)

Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Source: NIST, SP 800-53, Revision 5)

Configuration Management. A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development lifecycle. (Source: NIST, SP 800-53, Revision 5)

Control Assessment. The testing or evaluation of the controls in an information system or an organization 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 or privacy requirements for the system or the organization. (Source: NIST, SP 800-37, Revision 2)

Control Baseline. Predefined sets of controls specifically assembled to address the protection needs of groups, organizations, or communities of interest. See privacy control baseline or security control baseline. (Source: NIST, SP 800-53, Revision 5)

Controlled Unclassified Information (CUI). Information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Governmentwide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. (Adapted from: NIST, SP 800-53, Revision 5)

Data Integrity Board (DIB).

a. Every agency conducting or participating in a matching program shall establish a DIB to oversee and coordinate among the various components of such agency the agency's implementation of this section.

b. Each DIB shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the DIB.

c. Each DIB:

(1) Shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with 5 U.S.C. 552a Subsection (o), *Matching Agreements*, and all relevant statutes, regulations, and guidelines;

(2) Shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs; and

(3) Shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures.

(Source: *Privacy Act of 1974*, 5 U.S.C. § 552a)

Enterprise. An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks

and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information, and mission management. (Source: CNSS, CNSS Instruction (CNSSI)-4009, *Committee on National Security Systems (CNSS) Glossary*)

Enterprise Architecture. A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan. (Source: NIST, SP 800-53, Revision 5)

External Information System (or Component). An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (Source: CNSS, CNSSI-4009)

Firmware. Computer programs and data stored in hardware – typically in read-only memory (ROM) or programmable read-only memory (PROM) – such that the programs and data cannot be dynamically written or modified during execution of the programs. See hardware and software. (Source: NIST, SP 800-53, Revision 5)

Hardware. The material physical components of a system. See software and firmware. (Source: NIST, SP 800-53, Revision 5)

Hybrid Security Control. A security control that is implemented in an information system in part as a common control and in part as a system-specific control. (Source: OMB, A-130)

Impact. The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or a system. (Source: NIST, SP 800-53, Revision 5)

Incident. An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (Source: NIST, SP 800-53, Revision 5)

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: NIST, SP 800-53, Revision 5)

Information Technology (IT). Any services, equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency. For purposes of this definition,

such services or equipment if used by the agency directly or is used by a contractor under a contract with the agency [the Department] that requires its use; or to a significant extent, its use in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including cloud computing and help-desk services or other professional services which support any point of the lifecycle of the equipment or service), and related resources. Information technology does not include any equipment that is acquired by a contractor incidental to a contract which does not require its use. (Source: Adapted from: 40 U.S.C. § 11101, *Definitions*)

Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (Source: NIST, SP 800-53, Revision 5)

Media. Physical devices or writing surfaces including magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips, and printouts (but excluding display media) onto which information is recorded, stored, or printed within a system. (Source: NIST, SP 800-53, Revision 5)

Network. A system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (Source: NIST, SP 800-53, Revision 5)

Non-repudiation. Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message. (Source: NIST, SP 800-53, Revision 5)

Organization. An entity of any size, complexity, or positioning within an organizational structure, including Federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements. (Source: NIST, SP 800-53, Revision 5)

Overlay. A specification of security or privacy controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems. See tailoring. (Source: NIST, SP 800-53, Revision 5)

Personally Identifiable Information (PII). Any information about an individual maintained by an agency, including:

a. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

(Source: NIST, SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*)

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. (Source: OMB, Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*)

Potential Impact. The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect (FIPS PUB 199 low); a serious adverse effect (FIPS PUB 199 moderate); or a severe or catastrophic adverse effect (FIPS PUB 199 high) on organizational operations, organizational assets, or individuals. (Source: NIST, SP 800-53, Revision 5)

Records. All recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them. (Source: NIST, SP 800-53, Revision 5)

Residual Risk. Portion of risk remaining after security measures have been applied. (Source: CNSS, CNSSI-4009)

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

a. The adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and

b. The likelihood of occurrence.

(Source: NIST, SP 800-53, Revision 5)

Risk Assessment. The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. (Source: NIST, SP 800-53, Revision 5)

Risk Management. The program and supporting processes to manage risk to agency operations (including mission, functions, image, reputation), agency assets, individuals, other organizations, and the Nation, and includes establishing the context for risk-related activities; assessing risk; responding to risk once determined; and monitoring risk over time. (Source: NIST, SP 800-53, Revision 5)

Risk Mitigation. Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. (Source: NIST, SP 800-53, Revision 5)

Security. A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the organization's risk management approach. (Source: NIST, SP 800-53, Revision 5)

Security Control Assessment. The testing or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization. (Source: NIST, SP 800-30, Revision 1)

Security Assessment Report (SAR). Provides a disciplined and structured approach for documenting the findings of the assessor and the recommendations for correcting any identified vulnerabilities in the security controls. (Source: CNSS, CNSSI-4009)

Security Categorization. The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSSI-1253, *Categorization and Control Selection for National Security Systems* and in FIPS PUB 199 for other than national security systems. (Source: NIST, SP 800-53, Revision 5)

Security Category. The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation. (Source: NIST, SP 800-53, Revision 5)

Security Control. The safeguards or countermeasure prescribed for an information system, or an organization to protect the confidentiality, integrity, and availability of the system and its information. (Source: OMB, A-130)

Security Control Assessor (SCA). The individual, group, or organization responsible for conducting a security or privacy assessment. (Source: NIST, SP 800-39)

Security Control Baseline. The set of minimum-security controls defined for a low-impact, moderate-impact, or high-impact information system. (Source: NIST, SP 800-53, Revision 5)

Security Policy. A set of rules that governs all aspects of security-relevant system and system component behavior. (Source: NIST, SP 800-53, Revision 5)

Security Requirement. A requirement levied on an information system or an organization that is derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted. (Source: NIST, SP 800-37, Revision 2)

Sensitive Information. 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 5 U.S.C. Section 552a (the *Privacy Act*), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (Source: NIST, SP 800-150, *Guide to Cyber Threat Information Sharing*)

Software. Computer programs and associated data that may be dynamically written or modified during execution. (Source: NIST, SP 800-53, Revision 5)

Supply Chain. Linked set of resources and processes between and among multiple tiers of organizations, each of which is an acquirer, that begins with the sourcing of products and services and extends through their lifecycle. (Source: NIST, SP 800-53, Revision 5)

System Development Lifecycle. The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation, and maintenance, and ultimately its disposal that instigates another system initiation. (Source: NIST, SP 800-37, Revision 2)

System Owner (or Program Manager). Official responsible for the overall procurement, development, integration, modification, operation, and maintenance of a system. (Source: NIST, SP 800-53, Revision 5)

System Security Plan (SSP). Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (Source: NIST, SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*)

System-Specific Security Control. A security control for an information system that has not been designated as a common control or the portion of a hybrid control that is to be implemented within an information system. (Source: NIST, SP 800-30, Revision 1)

Tailored Control Baseline. A set of controls resulting from the application of tailoring guidance to a control baseline. (Source: NIST, SP 800-53, Revision 5)

Tailoring. The process by which security control baselines are modified by: identifying and designating common controls, applying scoping considerations on the applicability and

implementation of baseline controls, selecting compensating security controls, assigning specific values to organization-defined security control parameters, supplementing baselines with additional security controls or control enhancements, and providing additional specification information for control implementation. (Source: NIST, SP 800-53, Revision 5)

Threat. Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (Source: NIST, SP 800-53, Revision 5)

User. Individual, or (system) process acting on behalf of an individual, authorized to access a system. (Source: NIST, SP 800-53, Revision 5)

Vulnerability. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Source: NIST, SP 800-53, Revision 5)

APPENDIX C

AUTHORITIES AND REFERENCES

Atomic Energy Act of 1954, Public Law (P.L.) 83-703, August 30, 1954, as amended through P.L. 117-81, December 27, 2022, as amended

Chief Information Officer, 7 CFR § 2.32, as amended

Clinger-Cohen Act of 1996, P.L. 104-106, February 10, 1996, as amended

CNSS, CNSSI-1253, *Categorization and Control Selection for National Security Systems*, July 29, 2022

CNSS, CNSSI-4009, *Committee on National Security Systems Glossary*, March 2, 2022

CNSS, *Introducing the CNSS Library* website

Computer Fraud and Abuse Act of 1986, P.L. 99-474, October 16, 1986, as amended

Cybersecurity Act of 2015, P.L. 114-113, December 18, 2015, as amended

Definitions, 40 U.S.C. § 11101

E-Government Act of 2002, P.L. 107-347, December 17, 2002

Electronic Communications Privacy Act of 1986, P.L. 99-508, October 21, 1986

E.O. 13526, *Classified National Security Information*, December 29, 2009

E.O. 14028, *Improving the Nation's Cybersecurity*, May 12, 2021

Federal Agency Responsibilities, 44 U.S.C. § 3506(b)(2), January 3, 2012, as amended

Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §§ 3551, *et seq.*, December 18, 2014, as amended

FITARA [Federal Information Technology Acquisition Reform Act] Enhancement Act of 2017, P.L 115-88, November 21, 2017, as amended

Federal Register website

National Cybersecurity Protection Act of 2014, P.L. 113-282, December 18, 2014, as amended

NIST, FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001, change notices to December 3, 2002, as amended

NIST, FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, as amended

NIST, FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, as amended

NIST, FIPS PUB 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022, as amended

NIST, SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, September 2012, as amended

NIST, SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018, as amended

NIST, SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011, as amended

NIST, SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of December 10, 2020, as amended

NIST, SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, January 2022, as amended

NIST, SP 800-53B, *Control Baselines for Information Systems and Organizations*, October 2020, as amended

NIST, SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008, as amended

NIST, SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010, as amended

NIST, SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011, as amended

NIST, SP 800-150, *Guide to Cyber Threat Information Sharing*, October 2016, as amended

NIST, SP 800-171, Revision 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, February 2020, as amended

NIST, SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*, February 2021, as amended

Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch,* 5 CFR §§ 2635, *et seq*.

OMB, Circular A-11, *Preparation, Submission, and Execution of the Budget*, August 2023, as amended

OMB, Circular A-108, *Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act*, July 1, 1975, as amended

OMB, Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, as amended

OMB, Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001

OMB, Memorandum M-15-14, *Management and Oversight of Federal Information Technology*, June 10, 2015

OMB, Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*, August 10, 2021

OMB, Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021

OMB, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022

Paperwork Reduction Act of 1995, P.L. 104-13, May 22, 1995, as amended

Privacy Act of 1974, 5 U.S.C. § 552a, December 31, 1974, as amended

USDA, DR 1800-001, *Incident Preparedness, Response, and Recovery*, February 9, 2022, as amended

USDA, DR 3080-001, *Records Management*, May 16, 2016, as amended

USDA, DR 3130-013, *Information Technology Capital Planning and Investment Control*, May 24, 2021, as amended

USDA, DR 3145-001, *Oversight and Management of the Federal Information Technology Acquisition Reform Act (FITARA)*, May 7, 2021, as amended

USDA, DR 3170-001, *End User Workstation Configurations*, October 13, 2022, as amended

USDA, DR 3180-001, *Information Technology Standards*, January 5, 2021, as amended

USDA, DR 3185-001, *Enterprise Architecture*, April 19, 2022, as amended

USDA, DR 3440-003, *Controlled Unclassified Information (CUI) Program*, September 13, 2021, as amended

USDA, DR 3450-001, *Computer Matching Program Involving Personally Identifiable Information*, October 29, 2020, as amended

USDA, DR 3505-003, *Access Control for Information and Information Systems*, July 17, 2019, as amended

USDA, DR 3505-005, *Cybersecurity Incident Management*, November 30, 2018, as amended

USDA, DR 3515-002, *Privacy Policy and Compliance for Personally Identifiable Information (PII)*, October 30, 2020, as amended

USDA, DR 3540-003, *Security Assessment and Authorization*, August 12, 2014, as amended

USDA, DR 3545-001, *Information Security Awareness (ISA) Program*, October 25, 2023, as amended

USDA, DR 3565-003, *Plan of Action and Milestones Policy*, September 25, 2013, as amended

USDA, DR 3650-001, *Cloud Computing*, May 24, 2023, as amended

USDA, DR 4070-735-001, *Employee Responsibilities and Conduct*, October 4, 2007, as amended

USDA, *Information Technology (IT) Security Controls Baselines* SharePoint site