

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

DEPARTMENTAL REGULATION	NUMBER: DR 3600-003
SUBJECT: Robotic Process Automation (RPA) Policy	DATE: May 16, 2022
OPI: Office of the Chief Information Officer, Digital Infrastructure Services Center	EXPIRATION DATE: May 16, 2027

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	2
3. Scope	2
4. Policy	2
5. Roles and Responsibilities	5
6. Policy Exceptions	9
7. Inquiries	10
Appendix A – Acronyms and Abbreviations	A-1
Appendix B – Definitions	B-1
Appendix C – Authorities and References	C-1

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy for implementing the Office of Management and Budget (OMB) Memorandum [M-18-23](#), *Shifting From Low-Value to High-Value Work* across the USDA. It addresses the establishment of Robotic Process Automation (RPA) through the Center of Excellence (CoE) within the USDA Office of the Chief Information Officer (OCIO).
- b. RPA tools are software programs designed to interact with existing applications and automate routine rules-based tasks by mimicking user interactions. RPA tools reduce the burden of repetitive, simple tasks on employees, and have the potential to save time and taxpayer dollars, improve accuracy and productivity, ensure standardization and consistency of service, and free Federal employees to focus on more meaningful and analytical work.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy creates the basic framework for RPA at USDA.
- b. This policy may reference and mandate compliance with other directives. Compliance with such policies must defer to, and be superseded by, any prevailing or more recent Acts of Congress, Executive Orders, Presidential Policy Directives (PPD), and OMB memoranda, circulars, and guidance.
- c. This policy supports the OMB, [*The President's Management Agenda*](#) (PMA), which focuses on the modernization of the Federal workforce.

3. SCOPE

This policy applies to all USDA RPA capable processes and systems in USDA, and to Mission Areas, agencies, staff offices, contractors, grantees, and others working for or on behalf of USDA.

4. POLICY

- a. All USDA RPA development systems must adopt the RPA CoE development model.
- b. USDA RPA services must comply with all current Federal laws, USDA Information Technology (IT) security and risk management policies, and OCIO acquisition approval.
- c. USDA RPA services must comply with all Federal and Departmental privacy requirements, regulations, and policies, which will be reviewed periodically to align with changing the IT landscape and incorporate process and policy improvements.
- d. USDA RPA service acquisition vehicles must include Service Level Agreements (SLA) with clear, concise, and detailed language identifying the Service Provider responsibilities for accommodating *Federal Information Security Modernization Act* ([FISMA 2014](#)), and reporting and privacy management requirements per OMB Memorandum [M-21-02](#), *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*.
- e. USDA RPA services must comply with [DR 3180-001](#), *Information Technology Standards*.
- f. USDA RPA services must comply with the OCIO Information Security Center (ISC) Compliance and Policy Branch (CPB) standard operating procedure (SOP), [CPB-SOP-004](#), *USDA Seven-Step Risk Management Framework (RMF) Process Guide (USDA RMF)*.

- g. USDA RPA services must comply with [DR 3540-003](#), *Security Assessment and Authorization [A&A]*, and the [CPB Guidance Memo](#), *Fiscal Year (FY) 2020 Security Assessment and Authorization (A&A) Guidance*.
- h. USDA RPA services, including applications and functions residing on local computers and Departmental, Mission Area, agency, and staff office infrastructure, must use mature agile methodology as well as development, security, and operations (DevSecOps) best practices per USDA RPA CoE strategy.
- i. USDA RPA CoE strategy further provides that Mission Area, agency, and staff office IT staff should become familiar with lean product management, agile development, continuous delivery, and automated infrastructure at the team and program level as part of any modernization plan. Additionally, non-IT staff supporting privacy, security, and procurement should receive training in the multiple core disciplines outlined above. Sustained progress in these staff training areas is foundational to the successful implementation of new automation (RPA) efforts.
- j. USDA RPA Program Office governs both Centralized and Federated Center of Excellence (CoE) operational models. In the Centralized Model, the RPA CoE owns and manages the entire process for bot (a computer program that performs automatic repetitive tasks) intake, development, and production in coordination with the business area process owners. The Federated Model business area manages their intake, development, and production with RPA CoE touchpoints at strategic integrals.
- k. All Mission Areas, agencies, and staff offices must contact the CoE at SMORPA@usda.gov for all new RPA adoption efforts.
- l. All Mission Areas, agencies, and staff offices must report all existing and new RPA solutions and services to the CoE , including Pilot Projects, Proof-of-Concept projects, training, and learning activities.
- m. All Mission Areas, agencies, and staff offices must develop RPA solutions using the Department's approved automation software suite.
- n. All Mission Areas, agencies, and staff offices must acquire the Department approved RPA licenses and operating environments via the OCIO Digital Infrastructure Service Center (DISC).
- o. All USDA RPA development projects must include the involvement of a Qualified Service Provider (QSP). Whether using the Federated or Centralized CoE model, developers must meet the following QSP criteria to ensure quality products to the Department. The following language must be part of any procurement for RPA Services:
 - (1) The vendor or contractor must demonstrate that at least one member of the contract development team working directly on USDA automation, possesses an RPA

Developer Advanced Certificate of Completion from the Department's approved software vendor to be considered a QSP. Note: Formal Federal Regulatory authority or industry standards have yet to establish a baseline for accreditation or competency.

- (2) The Certificate of Completion proves that the user has successfully passed the Department's approved software vendor's RPA Developer Exam. It demonstrates that the graduate has been tested on the Department's approved software vendor best practices and demonstrated their ability to develop a functional software robot.
- (3) The Certified Developer must be part of the development team. Managers and supervisors from the developer's employer do not satisfy this requirement.

p. Security

- (1) All new application development efforts will bring security to the application and infrastructure by incorporating modern software development best practices, such as continuous monitoring and accredited platforms.
- (2) All Mission Areas, agencies, and staff offices must abide by DR 3640-001, *Identity, Credential, and Access Management* [ICAM], according to OMB, [M-19-17](#), *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, to employ ICAM policies where applicable.
- (3) All Mission Areas, agencies, and staff offices will comply with the security requirements of the DISC.
- (4) USDA will expand its continuous diagnostic capabilities for RPA solutions.

q. Acquisition

- (1) All Mission Areas, agencies, and staff offices must comply with DR 3130-009, *Non-Major Information Technology (IT) Investments* for non-major investments and [DR 3130-010](#), *United States Department of Agriculture Enterprise Information Technology Governance*, and [DR 3130-008](#), *Definition of Major Information Technology Investments* for major investments to ensure successful outcomes that align with business needs while meeting approved costs, schedule, and performance goals.
- (2) All Mission Areas, agencies, and staff offices must employ high-quality IT cost estimation practices per [DR 3130-012](#), *Information Technology Cost Estimating*.
- (3) All Mission Areas, agencies, and staff offices must comply with IT capital planning and investment control (CPIC) practices per [DR 3130-013](#), *Information Technology Capital Planning and Investment Control*, and embrace Technology Business Management (TBM) framework per the *Introduction* and Section 7, *What is the*

Agency IT Portfolio Summary; Section 11, *What is the Major IT Business Case*; and Section 13, *How do IT Infrastructure, IT Security, and IT Management Standard Investments differ from Major Business Cases*, of the OMB, [FY 2021 IT Budget – Capital Planning Guidance](#).

- (4) All Mission Areas, agencies, and staff offices will improve the Authorization to Operate (ATO) process to modernize and adapt the process to the RPA landscape, eliminate duplication of efforts, take advantage of inheritable security controls, and innovate Departmental approaches to security authorization within RPA solutions.
- (5) All Mission Areas, agencies, and staff offices must refer to the Federal Chief Information Officer (CIO) Council guidance, [The Application Rationalization Playbook](#), for best practices to evaluate existing Departmental contracts and RPA solutions for applicability before acquiring or developing new services.
- (6) All Mission Areas, agencies, and staff offices must notify the RPA CoE for all RPA related acquisitions.
- (7) All Mission Areas, agencies, and staff offices must coordinate with the Office of Contracting and Procurement (OCP), [USDA Contracting Desk Book 3.2](#), to include clear, detailed SLAs and language in acquisition vehicles that protect the interests of USDA and allow for adequate administrative control, security monitoring, reporting, continuous visibility of assets, vendor performance measurements, clearly defined roles and responsibilities, remediation for non-compliance, and risk mitigation.
- (8) All Mission Areas, agencies, and staff offices must employ the practice of category management to, where possible, procure common goods and services as a Department to eliminate redundancies, increase efficiency, and deliver more value and savings per OMB, [M-19-13](#), *Category Management: Making Smarter Use of Common Contract Solutions and Practices*, and [DR 3107-001](#), *Management of USDA IT Enterprise Initiatives*.

5. ROLES AND RESPONSIBILITIES

a. The USDA CIO will:

- (1) Serve as the chief policy advisor to the Secretary on RPA policy;
- (2) Develop and maintain Departmentwide RPA policy for USDA; and
- (3) Ensure the Office of the General Counsel (OGC) is engaged for advice and counsel concerning the acquisition and offering of RPA services, when appropriate.

- b. The Associate Chief Information Officer (ACIO), DISC will:
- (1) Serve as Director of the USDA RPA CoE;
 - (2) Direct the USDA enterprise-class RPA service development;
 - (3) Implement and execute the necessary internal controls to proactively monitor, measure, audit, report, and enforce compliance with the provisions of the directive;
 - (4) Establish a Department-level RPA CoE to monitor, guide, and report all RPA activity at USDA;
 - (5) Design, develop, and implement networking architectures that provide DISC customers with the secure, multi-tenant, Platform as a Service (PaaS) infrastructure to deliver RPA services with 99.9% availability to Mission Areas, agencies, and staff offices;
 - (6) Use the RPA CoE to serve the Department for all day-to-day RPA adoption efforts;
 - (7) Ensure all new USDA RPA adoption efforts go through the RPA CoE to establish proper awareness and handling of enterprise RPA solutions;
 - (8) Serve as the RPA policy coordinator and technical advisor to the USDA CIO;
 - (9) Administer any certifications regarding RPA services and automation-based information systems that are required;
 - (10) Provide signature authority for routine RPA correspondence to Mission Areas, agencies, and staff offices from the OCIO; and
 - (11) Partner with Mission Areas, agencies, and staff offices to ensure the effective and efficient use of RPA services.
- c. The USDA Chief Information Security Officer (CISO), OCIO-ISC, will:
- (1) Advise the USDA CIO about strategies and methodologies for securing RPA services;
 - (2) Advise policy exception waiver requestors and reviewers on matters related to cybersecurity; and
 - (3) Improve the ATO process for RPA per DR 3540-003.
- d. The Departmental Chief Privacy Officer (CPO), OCIO-ISC-CPO, will ensure RPA service offerings comply with Federal and Departmental privacy requirements,

regulations, and policies, including [DR 3515-002](#), *Privacy Policy and Compliance for Personally Identifiable Information (PII)*.

- e. The ACIO, Information Resource Management Center (IRMC) will:
 - (1) Ensure RPA service offerings comply with Departmental Enterprise Information Technology Governance (EITG) and CPIC policies;
 - (2) Ensure RPA service offerings comply with Acquisition Approval Request (AAR) process, the *Federal Information Technology Acquisition Reform Act* (FITARA); OMB [M-12-10](#), *Implementing PortfolioStat*; and OMB [M-15-14](#), *Management and Oversight of Federal Information Technology*, Section C, *Transparency, Risk Management, Portfolio Review, and Reporting* for TechStat requirements;
 - (3) Ensure RPA service offerings comply with Federal and Departmental Section 508 requirements, regulations, and policies; and
 - (4) Ensure RPA service offerings comply with Federal and Departmental enterprise architecture (EA) regulations, policies, standards, and requirements.
- f. The USDA General Counsel will:
 - (1) Serve as the Departmental Freedom of Information Act (FOIA) Officer; and
 - (2) Ensure RPA service offerings comply with Federal [5 United States Code \(U.S.C.\) § 552](#), [DR 3450-002](#), *Freedom of Information Act Implementing Regulations* requirements and policies, and the regulations at [7 Code of Federal Regulations \(CFR\) Part 1](#), *Administrative Regulations*.
- g. Mission Area Assistant CIOs will:
 - (1) Ensure that their Mission Areas, agencies, and staff offices comply with this directive and other applicable Federal and USDA policies, regulations, and guidance regarding RPA;
 - (2) Ensure IT entities working for, or on behalf of, USDA understand their responsibilities when implementing RPA services;
 - (3) Ensure actions are taken to secure USDA information and information systems as required under Federal and USDA policies and guidance;
 - (4) Ensure that contract language for acquiring services addresses security monitoring, security auditing, and remediation of security concerns in accordance with Federal and USDA regulations and standards;

- (5) Record, track, and resolve all plans of action and milestones (POA&M) USDA CIO [DR 3565-003](#), *Plan of Action and Milestones Policy*, and [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1, November 2015, for RPA offerings in the USDA FISMA data management and reporting tool per DR 3540-003, *Security Assessment and Authorization*;
 - (6) Provide the USDA CIO with a written analysis annually on the progress of assuring IT systems to comply with this policy;
 - (7) Be responsive to RPA data calls and certifications as required; and
 - (8) Track and contain total cost of ownership expenditures for USDA RPA information systems.
- h. Mission Area, Agency, and Staff Office System Owners will:
- (1) Use the RPA CoE as the intake point for all RPA efforts including pilot projects and proof-of-concept projects;
 - (2) Ensure statements of work, SLAs, and procurement requests for all RPA acquisition contracts include requirements for providing USDA with a proper level of performance and continuous accountability, availability, awareness, policy compliance, confidentiality, and integrity of the IT assets and data handled by automation services per [DR 3520-002](#), *Configuration Management*;
 - (3) Ensure adequate budgeting for operating, managing, and scaling RPA as needed; and
 - (4) Document the configuration management and inventory management activities for RPA solutions.
- i. The Director, Office of Human Resource Management (OHRM), serving as the Chief Human Capital Officer (CHCO), will:
- (1) Collaborate with the USDA CIO and Chief Financial Officer (CFO) to periodically update the training and hiring practices to ensure the IT workforce has the skillsets needed to efficiently use RPA, and
 - (2) Work jointly with the USDA CIO to identify two top positions or skill segment priorities and incorporate them into the Department's Human Capital Operating Plan per [5 CFR Part 250](#), *Personnel Management in Agencies*, Federal CIO Council actions, and be consistent with the PMA.

- j. The USDA CFO will:
 - (1) Develop and implement strategies for shifting resources to high-value activities to eliminate unnecessary or obsolete compliance requirements and reduce the cost of mission-support operations, as required by OMB M-18-23; and
 - (2) Collaborate with the CIO and CHCO to periodically update the procurement and acquisition practices to ensure the Department has the capital planning and talent acquisition strategies suitable for effective RPA adoption.
- k. The Director, OCP, will ensure all RPA contracts align with the *Federal Acquisition Regulations* (FAR), [FAR Part 39](#), *Acquisition of Information Technology*.
- l. The Departmental Records Officer in the Office of Information Affairs in the Office of the General Counsel (OGC), will ensure RPA service offerings comply with Federal and Departmental records management, eDiscovery, litigation hold, and electronically stored information records retention requirements, regulations, and policies.
- m. Information Systems Security Managers (ISSM) will safeguard and maintain information systems within each Mission Area that RPA integrates, as required by Departmental Manual [\(DM\) 3545-002](#), *USDA Information Systems Security Program (ISSP)*.

6. POLICY EXCEPTIONS

All USDA Mission Areas, agencies, and staff offices are required to conform to this policy. The Mission Area Assistant CIOs, and Agency and Staff Office IT Directors, must submit a waiver request to the ACIO DISC for internal coordination and review on behalf of the USDA CIO if:

- a. A policy requirement cannot be met as explicitly stated; or
- b. Current USDA RPA CoE standards and offerings do not meet the mission needs;
- c. The waiver request must explain the reason for the request, identify compensating controls or actions that meet the policy's intent, and identify how the compensating controls or actions provide a comparable or greater level of defense or compliance than required by the policy; and
- d. Waivers approved by the USDA CIO must be associated with a National Institute of Standards and Technology (NIST), Special Publication [\(SP\) 800-53 \(Rev. 5\)](#), *Security and Privacy Controls for Information Systems and Organizations*, control, recorded, and tracked as a POA&M item in the USDA FISMA data management and reporting tool. Waivers will expire at the end of the FY or 6 months from the date of approval,

whichever is longer. Unless otherwise specified, Mission Areas, agencies, and staff offices must review and renew approved policy waivers every FY.

7. INQUIRIES

Inquiries about this policy must be directed to the ACIO DISC. Contact the ACIO DISC at SMORPA@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

A&A	Assessment and Authorization
AAR	Acquisition Approval Request
ACIO	Associate Chief Information Officer
ATO	Authorization to Operate
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CoE	Center of Excellence
CPB	Compliance and Policy Branch (OCIO-ISC Component)
CPIC	Capital Planning and Investment Control
CPO	Chief Privacy Officer
DevSecOps	Development, Security, and Operations
DHS	Department of Homeland Security
DISC	Digital Infrastructure Services Center (OCIO Component)
DM	Departmental Management
DR	Departmental Regulation
EA	Enterprise Architecture
EITG	Enterprise Information Technology Governance
FAQ	Frequently Asked Question
FAR	Federal Acquisition Regulations
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GSA	General Services Administration
ICAM	Identity, Credential, and Access Management
IRMC	Information Management Resource Center (OCIO Component)
ISC	Information Security Center (OCIO Component)
ISSM	Information Systems Security Manager
IT	Information Technology
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OCP	Office of Contracting and Procurement
OGC	Office of the General Counsel
OHRM	Office of Human Resource Management
OMB	Office of Management and Budget

PaaS	Platform as a Service
P.L.	Public Law
PMA	President's Management Agenda
POA&M	Plan of Action and Milestones
PPD	Presidential Policy Directive
QSP	Qualified Service Provider
RMF	Risk Management Framework
RPA	Robotic Process Automation
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SP	Special Publication
TBM	Technology Business Management
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

Agile. An alternative approach to traditional project management or product development. It is a value-based, iterative approach under which requirements and solutions evolve through the collaborative effort of self-organizing cross-functional teams. Agile advocates adaptive planning, evolutionary development, early delivery, and continuous improvement, and it encourages rapid and flexible response to change. (Source: General Services Administration (GSA), [GSA Tech Guides, Agile Guides](#) website)

Bot. A computer program that performs automatic repetitive tasks. (Source: Merriam-Webster, [Dictionary](#) website, retrieved May 11, 2022)

Continuous Diagnostics and Mitigation (CDM). A CDM program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. CDM provides Federal departments and agencies with capabilities and tools that identify cybersecurity risk on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. (Source: Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), [Continuous Diagnostics and Mitigation \(CDM\)](#) website)

Contractor Support. Contractor support encompasses on-site or off-site contractor technical or other support staff. (Source: OMB, [M-12-20, FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management](#))

Development, Security, and Operations (DevSecOps). A cultural and engineering practice that breaks down barriers and opens collaboration between development, security, and operations organizations using automation to focus on rapid, frequent delivery of secure infrastructure and software to production. It encompasses intake to release of software and manages those flows predictably, transparently, and with minimal human intervention and effort. (Source: GSA, Tech Guides, [DevSecOps Guide](#))

Executive Agency. An executive department specified in [5 U.S.C. § 101](#), *Executive departments*; a military department specified in [5 U.S.C. § 102](#), *Military departments*; an independent establishment as defined in [5 U.S.C. § 104\(1\)](#), *Independent establishment*; and a wholly owned Government corporation fully subject to the provision of [31 U.S.C. Chapter 91](#), *Government Corporations*. (Source: [41 U.S.C. § 133](#), *Executive Agency*)

Federal Information System. An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (Source: [40 U.S.C. § 11331](#), *Responsibilities for Federal information system standards*)

Information. Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative,

contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive order, directive, policy, or regulation. (Source: NIST, Federal Information Processing Standards Publication ([FIPS PUB](#)) 199, *Standards for Security Categorization of Federal information and Information Systems*)

Information Resources. Information and related resources, such as personnel, equipment, funds, and information technology. (Source: [44 U.S.C. § 3502](#), *Definitions*)

Information Systems. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: 44 U.S.C. § 3502)

Information System Operated by a Contractor on Behalf of an Agency. An information system operated by a contractor on behalf of an agency must be treated in the same way as agency-operated information systems. The level of effort required for security authorization depends on the impact level of the information contained in the system. The security authorization boundary for these systems must be carefully mapped to ensure that Federal information (Source: OMB, M-12-20):

- a. Is adequately protected;
- b. Is segregated from the contractor, state, or grantee corporate infrastructure; and
- c. There is an interconnection security agreement in place to address connections from the contractor, state, or grantee system containing the agency information to systems external to the security authorization boundary.

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. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:

- a. Requires the use of such equipment; or
- b. Requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. (Source: [40 U.S.C. § 11101](#), *Definitions*)

PortfolioStat 2.0. Is a tool that agencies use to assess the current maturity of their IT portfolio management process, make decisions on eliminating duplication, augment current CIO-led CPIC processes, and move to shared solutions in order to maximize the return on IT investments across

the portfolio. (Source: OMB, [*PortfolioStat 2.0: Driving Better Management and Efficiency in Federal IT*](#))

Robotic Process Automation (RPA). RPA tools are software programs designed to interact with existing applications and automate routine rules-based tasks by mimicking user interactions. RPA tools reduce the burden of repetitive, simple tasks on employees, and have the potential to save time and taxpayer dollars, improve accuracy and productivity, ensure standardization and consistency of service, and free Federal employees to focus on more meaningful and analytical work. Additionally, RPA tools operate on existing information systems so agencies do not have to invest time and resources redesigning systems or refactoring applications. Therefore, RPA solutions tend to have lower implementation costs and lower risk than large IT transformations. (Source: Federal CIO Council, [*Robotic Process Automation in Federal Agencies*](#))

TechStat. Is a face-to-face, evidence-based accountability review of an IT investment for Federal agencies. (Source: OMB, [*TechStat: Improving Government Performance*](#))

APPENDIX C
AUTHORITIES AND REFERENCES

[5 CFR Part 250](#), *Personnel Management in Agencies*

[7 CFR Part 1](#), *Administrative Regulations*

[5 U.S.C. § 101](#), *Executive departments*

[5 U.S.C. § 102](#), *Military departments*

[5 U.S.C. § 104\(1\)](#), *Independent establishment*

[31 U.S.C. Chapter 91](#), *Government Corporations*

[40 U.S.C. § 11101](#), *Definitions*

[40 U.S.C. § 11331](#), *Responsibilities for Federal information system standards*

[41 U.S.C. § 133](#), *Executive Agency*

[44 U.S.C. § 3502](#), *Definitions*

Clinger-Cohen Act of 1996, [40 U.S.C. § 11101](#), *et seq.*, February 10, 1996

Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA), [Continuous Diagnostics and Mitigation \(CDM\)](#) website

Federal Acquisition Regulations (FAR), [FAR Part 39](#), *Acquisition of Information Technology*

Federal Chief Information Officer (CIO) Council, [The Application Rationalization Playbook](#), Version 1.1, June 18, 2019

Federal CIO Council, [Management and Oversight of Federal Information Technology Implementation Guide](#) website

Federal CIO Council, [Robotic Process Automation in Federal Agencies](#)

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

Federal Information Technology Acquisition Reform Act (FITARA), [P.L. 113-291, 128 Stat. 3292, Title VIII, Subtitle D, § 831-837](#), December 19, 2014

Freedom of Information Act (FOIA), [5 U.S.C. § 552](#)

GSA, [GSA Tech Guides, Agile Guides](#) website

GSA, [GSA Tech Guides, DevSecOps Guide](#) website

Merriam-Webster, [Dictionary](#) website

NIST, [FIPS PUB 199](#), *Standards for Security Categorization of Federal information and Information Systems*, February 2004

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

OMB, [FY 2021 IT Budget - Capital Planning Guidance](#), June 28, 2019, Technical Business Management

OMB, [M-12-10](#), *Implementing PortfolioStat*, March 30, 2012

OMB, [M-12-20](#), *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 27, 2012

OMB, [M-15-14](#), *Management and Oversight of Federal Information Technology*, June 10, 2015

OMB, [M-18-23](#), *Shifting From Low-Value to High-Value Work*, August 27, 2018

OMB, [M-19-02](#), *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 25, 2018

OMB, [M-19-13](#), *Category Management: Making Smarter Use of Common Contract Solutions and Practices*, March 20, 2019

OMB, [M-19-17](#), *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, May 21, 2019

OMB, [M-21-02](#), *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, November 9, 2020

OMB, [PortfolioStat 2.0: Driving Better Management and Efficiency in Federal IT](#), March 27, 2013

OMB, [The President's Management Agenda](#) webpage

OMB, [TechStat: Improving Government Performance](#), February 24, 2010

USDA, [DM 3545-002](#), *Information Systems Security Program*, March 31, 2006

USDA, [DR 3107-001](#), *Management of USDA IT Enterprise Initiatives*, May 12, 2016

USDA, [DR3130-008](#), *Definition of Major Information Technology Investments*, August 13, 2020

USDA, [DR 3130-009](#), *Non-Major Information Technology (IT) Investments*, September 28, 2020

USDA, [DR 3130-010](#), *United States Department of Agriculture Enterprise Information Technology Governance*, April 20, 2021

USDA, [DR 3130-012](#), *Information Technology Cost Estimating*, March 4, 2016

USDA, [DR 3130-013](#), *Information Technology Capital Planning and Investment Control*, May 24, 2021

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

USDA, [DR 3180-001](#), *Information Technology Network Standards*, January 5, 2021

USDA, [DR 3440-003](#), *Controlled Unclassified Information (CUI) Program*, September 13, 2021

USDA, [DR 3445-001](#), *Media Protection*, October 30, 2019

USDA, [DR 3450-002](#), *Freedom of Information Act Implementing Regulations*, February 7, 2003

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

USDA, [DR 3520-002](#), *Configuration Management*, August 14, 2014

USDA, [DR 3540-003](#), *Security Assessment and Authorization*, August 12, 2014

USDA, [DR 3565-003](#), *Plan of Action and Milestones Policy*, September 25, 2013

USDA, [DR 3640-001](#), *Identity, Credential, and Access Management*, June 8, 2021

USDA, [DR 4030-001](#), *Section 508*, September 8, 2014

USDA, [Integrated Information Technology Governance Framework](#)

USDA, OCIO, ISC, [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1, November 2015

USDA, OCIO, ISC, [CPB Guidance Memo](#), *Fiscal Year (FY) 2020 Security Assessment and Authorization (A&A) Guidance*, September 2020

USDA, [OCIO, ISC, CPB-SOP-004, Revision 4](#), *USDA Seven Step Risk Management Framework (RMF) Process Guide* (USDA RMF), September 2019

USDA, OCP, [Contracting Desk Book 3.2](#), April 4, 2022