

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

DEPARTMENTAL REGULATION	NUMBER: DR 3650-001
SUBJECT: Cloud Computing	DATE: January 22, 2025
OPI: Office of the Chief Information Officer, Digital Infrastructure Services Center	EXPIRATION DATE: January 22, 2030

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Scope	2
3. Special Instructions/Cancellations	2
4. Policy	2
5. Roles and Responsibilities	6
6. Policy Exceptions	12
7. Inquiries	12
Appendix A – Acronyms and Abbreviations	A-1
Appendix B – Definitions	B-1
Appendix C – Authorities and References	C-1

1. PURPOSE

This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy for cloud computing and supports modern approaches, guidance, and requirements for cloud computing, as outlined by:

- a. Applicable laws enacted by the United States Congress;
- b. Executive Orders (E.O.) issued by the President of the United States;
- c. Office of Management and Budget (OMB) cloud policies, including OMB memorandums such as, [M- 19-13](#), *Category Management: Making Smarter Use of Common Contract Solutions and Practices*;
- d. The cloud service standards authored by the National Institute of Standards and Technology (NIST) and the Cybersecurity and Infrastructure Security Agency (CISA);

- e. The 2019 [Cloud Smart](#) Federal cloud computing strategy;
- f. All applicable USDA directives, such as those in Appendix C; and
- g. USDA [Strategic Plan Fiscal Years 2022-2026](#), Objective 6.3: Promote USDA Operational Excellence Through Better Use of Technology and Shared Solutions.

2. SCOPE

- a. This DR applies to any USDA information system operated by the Office of the Chief Information Officer (OCIO), Mission Areas, agencies, staff offices, and any entity or person working for or on behalf of USDA.
- b. This DR applies to all USDA cloud-capable information systems in USDA's information systems portfolio.
- c. All USDA cloud-capable information systems fall under the NIST definition of "cloud computing" as outlined in NIST [Special Publication \(SP\) 800-145](#), *The NIST Definition of Cloud Computing*.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR supersedes DR 3650-001, *Cloud Computing*, dated May 24, 2023.
- b. This DR does not apply to classified national security information.
- c. This DR adheres to the guidance in NIST [SP 800-53](#), Revision 5, *Security and Privacy Controls for Information Systems and Organizations*. It also adheres to the guidance in NIST [Federal Information Processing Standards Publication \(FIPS PUB\) 199](#), *Standards for Security Categorization of Federal Information and Information Systems*.
- d. In December 2022, the *FedRAMP Authorization Act* was signed as part of the *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, [Public Law \(P.L.\) 117-263, as amended through P.L. 118-31](#). The *FedRAMP Authorization Act* codifies the Federal Risk and Authorization Management Program (FedRAMP) as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information.

4. POLICY

- a. Cloud computing is the primary approach to transforming how the USDA delivers, protects, and manages access to data and applications across all Mission Areas, agencies, and staff offices. Cloud computing will be implemented to maximize advantages including but not limited to cyber compliance, increased administrative efficiency, elasticity and scalability, central access, and transparent cost.
- b. The USDA cloud computing environment ensures effective support for the full range of missions and data classifications with a purposefully orchestrated multi-cloud, multi-vendor strategy. This strategy focuses on limiting duplication, reducing inefficiencies, and accelerating digital modernization efforts.
- c. All new software and software development will leverage the inherent characteristics of cloud computing services, maximize use of cloud services, and support continuous integration and continuous delivery to the maximum extent possible that both mission requirements and technical capabilities allow.
- d. USDA will adopt the Cloud Smart strategies.
- e. Cloud computing services must comply with all current Federal laws and USDA information technology (IT) security, privacy, and risk management policies.
- f. Cloud computing service acquisition vehicles must include service level agreements (SLA). These SLAs must have clear, concise, and detailed language identifying the cloud computing source responsibilities for accommodating the reporting and privacy management requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), [44 United States Code \(U.S.C.\) § 3551, et seq.](#) This must be done per OMB [M-24-04](#), *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*.
- g. As directed by [E.O. 14028](#), *Improving the Nation's Cybersecurity*, Federal Agencies migrating to cloud deployments must apply zero trust principles and transition their environments to Zero Trust architectures commensurate with their risk tolerance. For more information on zero trust, see NIST [Cybersecurity White Paper \(CSWP\) 20](#), *Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators*.
- h. Cloud computing services must comply with [DR 3180-001](#), *Information Technology Standards*.
- i. Cloud computing services must comply with NIST [SP 800-37](#), Revision 2, *Risk Management Framework (RMF) for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Cloud computing services must also comply with the associated OCIO Cybersecurity and Privacy Operations Center (CPOC) [Risk Management Framework 2.0](#), as amended.

- j. Cloud computing services must comply with [DR 3540-003](#), *Security Assessment and Authorization*.
- k. Cloud computing services must comply with policy and procedures in [DR 3520-002](#), *Configuration Management*.
- l. All Mission Areas, agencies, and staff offices must register and report all existing and new cloud systems and services to the USDA [Enterprise Architecture Vision Environment](#) (EAVE). To do this, please contact your Mission Area Assistant Chief Information Officer (CIO) or Mission Area, agency, or staff office enterprise architect.

5. SECURITY

- (1) All new application development efforts will bring security to the application and data layer by incorporating modern software development best practices, such as continuous monitoring and zero trust.
- (2) All Mission Areas, agencies, and staff offices must abide by [DR 3640-001](#), *Identity, Credential, and Access Management*, pursuant to OMB [M-19-17](#), *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, to employ identity, credential, and access management policies where applicable.
- (3) USDA will expand its continuous diagnostic capabilities for cloud environments per the Department of Homeland Security's (DHS) [Continuous Diagnostics and Mitigation Program](#).
- (4) As stated in E.O. 14028, Section 3(c): "As [Federal] agencies continue to use cloud technology, they shall do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology will adopt Zero Trust Architecture, as practicable."
- (5) USDA cloud authorizations to operate (ATO) based on FedRAMP have two types:
 - (a) FedRAMP ATOs that are specific to Mission Areas, agencies, or staff offices that support a single USDA Mission Area, agency, or staff office under the Associate Chief Information Officer (ACIO) as the Authorizing Official and System Owner; and
 - (b) Enterprise FedRAMP ATOs that support two or more Mission Areas, agencies, or staff offices under the OCIO Digital Infrastructure Services Center (DISC) ACIO as the Authorizing Official and System Owner.

6. ACQUISITION

- a. All Mission Areas, agencies, and staff offices must comply with Section 834(c) of the *Federal Information Technology Acquisition Reform Act* (FITARA), [P.L. 113-291, Title VIII, Subtitle D, Sections 831-837](#). They must comply with this by adhering to [DR 3145-001](#), *Oversight and Management of the Federal Information Technology Acquisition Reform Act (FITARA)*, and OMB [M-15-14](#) (CTO) need to give documented approval of an IT purchase to remain compliant with the guidance on the GSA Technology Transformation Service (TTS) Handbook's web page [Federal Information Technology Acquisition Reform Act \(FITARA\)](#).
- b. All Mission Areas, agencies, and staff offices must comply with [DR 3130-009](#), *Non-Major Information Technology (IT) Investments*, for non-major investments. They must comply with [DR 3130-010](#), *United States Department of Agriculture Enterprise Information Technology Governance*, for major investments. This will ensure successful outcomes that align with business needs while meeting approved costs, schedule, and performance goals.
- c. All Mission Areas, agencies, and staff offices must employ high-quality IT cost estimation practices per [DR 3130-012](#), *Information Technology Cost Estimating*.
- d. 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*. They must embrace the Technology Business Management (TBM) framework per the introduction and Sections 7, 11, and 13 of OMB's *FY 2021 IT Budget – Capital Planning Guidance*.
- e. All Mission Areas, agencies, and staff offices will refer to the Federal CIO Council's [The Application Rationalization Playbook](#) for best practices in evaluating existing Departmental contracts and cloud computing solutions before acquiring or developing new acquisition strategies or acquisition plans for services.
- f. For any acquisitions related to cloud services, USDA personnel must evaluate and consider the available USDA STRATUS cloud acquisition vehicles. They must incorporate this evaluation into the cloud abbreviated acquisition plan. They will generate an analysis of alternatives and make it available to the STRATUS program office. The order of precedence for procuring authorized cloud services is as follows:
 - (1) A FedRAMP-authorized cloud service provider (CSP);
 - (2) An existing USDA authorization to operate (ATO) for commercial cloud services; and
 - (3) Sponsorship of a CSP for FedRAMP authorization through the initial Federal Agency authorization process.

- g. All Mission Areas, agencies, and staff offices must coordinate with the Director of the Office of Contracting and Procurement (OCP) to include the appropriate SLAs and language in acquisition vehicles. For example, acquisition vehicles must comply with USDA policy, as well as Section 508, E.O.s, and other Federal guidance. Using appropriate language protects the interests of USDA and allows for adequate administrative control, security monitoring, reporting, continuous visibility of assets, vendor performance measurements, clearly defined roles and responsibilities, remediation for noncompliance, and risk mitigation.
- h. All Mission Areas, agencies, and staff offices must follow the practice of category management and adhere to [DR 3160-001](#), *Licensed Information Technology (IT) Software*, to procure common goods and services. Where possible, seek to eliminate redundancies, increase efficiency, and deliver more value and savings, per M-19-13, M-22-03, and [DR 3107-001](#), *Management of USDA IT Enterprise Initiatives*.

7. ROLES AND RESPONSIBILITIES

- a. The USDA CIO will:
 - (1) Serve as the chief policy advisor to the Secretary on cloud computing policy;
 - (2) Develop and maintain Departmentwide policy for USDA information systems operating on CSP offerings;
 - (3) Direct the USDA enterprise private cloud service development;
 - (4) Enforce compliance with the provisions of this policy;
 - (5) Review and be the final decision authority for all policy waiver requests (as explained in Section 6: Policy Exceptions);
 - (6) Collaborate with the Director of the Office of Human Resource Management (OHRM), who serves as the Chief Human Capital Officer (CHCO), and the Chief Financial Officer (CFO) to periodically update the training and hiring practices;
 - (7) Provide to the Federal CIO annually a written list of all cloud services that the Department has determined cannot meet or are not required to meet FedRAMP security authorization requirements, and ensure that the list is jointly signed by the USDA CIO and CFO;
 - (8) Ensure that the General Counsel is engaged for advice and counsel with respect to the acquisition and offering of cloud services, when appropriate; and

- (9) Work with other parts of the Department, namely the CFO, the Director of OHRM, and the Director of OCP, to best align procurement and workforce management practices to cloud computing.
- b. The USDA CTO will:
 - (1) Review policy waiver requests and provide recommendations to the CIO; and
 - (2) Give documented approval of an IT purchase, in agreement with the CIO, to remain compliant with the guidance of GSA *TTS Handbook*'s web page *Federal Information Technology Acquisition Reform Act (FITARA)*.
- c. The DISC ACIO will:
 - (1) Serve as the Departmental Cloud Broker as described in NIST [SP 500-291](#), Version 2, *NIST Cloud Computing Standards Roadmap*, Section 4.5: Cloud Broker;
 - (2) Serve as the cloud computing policy coordinator and technical advisor to the USDA CIO;
 - (3) Develop and maintain the process for exceptions to this policy;
 - (4) Review policy waiver requests and provide recommendations to the CIO;
 - (5) Be the delegated signature authority for cloud computing correspondence from the CIO to Mission Areas, agencies, and staff offices;
 - (6) Partner with Mission Areas, agencies, and staff offices to ensure the effective and efficient use of cloud services;
 - (7) Maintain oversight and report to the CIO on the program compliance status of USDA in commercial cloud deployments;
 - (8) Authorize and maintain for use enterprise FedRAMP commercial CSP ATOs;
 - (9) Direct the Security Governance Division to maintain USDA cybersecurity assessment and management activities as necessary, ensuring the inheritance of security controls from enterprise FedRAMP commercial CSP ATOs; and
 - (10) Engage in continuous monitoring of enterprise FedRAMP commercial CSPs as prescribed by FedRAMP.
- d. The DISC Enterprise Architect will:

- (1) Be responsible for the design and architecture of USDA's cloud program services and infrastructure;
 - (2) Ensure that cloud services align with the requirements of the USDA [*Information Technology Strategic Plan 2022-2026*](#);
 - (3) Ensure that cloud services comply with USDA's enterprise architecture requirements;
 - (4) Select CSPs;
 - (5) Facilitate collaboration through USDA's Cloud Working Group between the Cloud Broker, Cloud Carrier, and System Owners; and
 - (6) Ensure that cloud services are integrated with USDA's existing infrastructure.
- e. The Director of DISC's Enterprise Network Division will:
- (1) Serve as Cloud Carrier, per NIST SP 500-291, Version 2, Section 4.6: Cloud Carrier;
 - (2) Design, develop, and implement networking architectures that provide CSPs with the necessary connectivity, availability, bandwidth, and latency to deliver cloud services to Mission Areas, agencies, and staff offices;
 - (3) Require CSPs to meet the requirements of Trusted Internet Connection (TIC) 3, consistent with DHS guidance and Zero Trust Architecture;
 - (4) Manage all domain name systems (DNS) as required by [*DR 3300-025, Secure Domain Name System*](#), and any domain name system security extensions (DNSSEC) for the CSPs as part of the USDA enterprise network.
- f. The Chief Information Security Officer (CISO) and CPOC's ACIO will:
- (1) Review policy waiver requests and provide recommendations to the CIO;
 - (2) Advise the CIO about cybersecurity strategies and methodologies for securing USDA commercial cloud services;
 - (3) Maintain oversight and report to the CIO on the cybersecurity compliance status of USDA in commercial cloud deployments; and
 - (4) Lead the USDA cybersecurity risk management program and serve as a deciding official for enterprise wide, cybersecurity risk-based decisions per [*Risk Based Decision \(RBD\) Standard Operating Procedure \(SOP\) RBD-SOP-3540-003B*](#),

Revision 1.6, *USDA Standard Operating Procedures on Risk-Based Decision Management*.

- g. The Branch Chief of CPOC's Risk Management Branch will:
- (1) Determine whether CSP offerings have an acceptable risk level under the [Impact-Level Prioritization](#) web page of USDA's *Risk Management Framework 2.0* website;
 - (2) Approve plans of action and milestones (POA&M) for the CSP offerings determined not to have an acceptable risk level under USDA's *Impact-Level Prioritization* web page;
 - (3) Ensure that Departmental CSPs complete security monitoring, security auditing, and remediation of security concerns in accordance with Federal and Departmental guidelines;
 - (4) Ensure continuous monitoring, continuous security operations, and disaster recovery of USDA IT systems and networks, where possible; and
 - (5) Monitor policy compliance and policy exception waivers and report cloud policy deviations to the CIO within 10 business days of discovery for resolution.
- h. The Chief Privacy Officer will ensure that cloud service offerings comply with Federal and Departmental privacy requirements, regulations, and policies, including [DR 3445-001](#), *Media Protection*.
- i. The ACIO of OCIO's Information Resource Management Center (IRMC) will:
- (1) Ensure that cloud service investments comply with Departmental enterprise IT governance and CPIC policies, including DR 3130-010, DR 3130-013, and DR 3145-001;
 - (2) Ensure that cloud service investments comply with the requirements of acquisition approval requests (AAR), FITARA, OMB's PortfolioStat (see CIO.gov's web page [6.2 PortfolioStat](#)), and OMB's TechStat (see CIO.gov's web page [6.3 TechStat](#));
 - (3) Ensure that cloud service deployments comply with the standards, requirements, regulations, and policies of Federal and Departmental Section 508 and Web Content Accessibility Guidelines (WCAG; see the World Wide Web Consortium [W3C] website [WCAG 2 Overview](#)). This must occur per [DR 4030-001](#), *Section 508 Program*;
 - (4) Ensure that cloud service deployments comply with Federal and Departmental enterprise architecture regulations, policies, standards, and requirements. USDA requirements include [DR 3185-001](#), *Enterprise Architecture*; [DR 3185-002](#),

Enterprise Architecture IT Asset Definitions; and [DR 3185-003](#), Enterprise Architecture IT Asset Data Element Requirements; and

- (5) Ensure that cloud service deployments comply with Federal and Departmental controlled unclassified information (CUI) regulations, policies, standards, and requirements per [DR 3440-003](#), *Controlled Unclassified Information (CUI) Program*.
- j. Mission Area Assistant CIOs will:
- (1) Ensure that their Mission Areas, agencies, and staff offices comply with this DR and other applicable Federal and USDA policies, regulations, and guidance regarding cloud computing;
 - (2) Ensure that staff working for or on behalf of USDA understand their responsibilities when implementing cloud computing services as the Cloud Consumer, per NIST SP 500-291, Version 2, Section 4.2: Cloud Consumer;
 - (3) Identify Mission Area, agency, and staff office personnel who are Information Systems Security Managers, and task them with ensuring that CSPs are in full compliance with FISMA; NIST FIPS PUB 199; and NIST [SP 800-60](#), Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*;
 - (4) Ensure that actions are taken to secure USDA information and information systems as required under Federal and USDA policies and guidance;
 - (5) 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;
 - (6) Record, track, and resolve all POA&Ms for CSP deployments in the USDA FISMA data management and reporting tool;
 - (7) Provide the CIO with a written analysis each fiscal year (FY) on the progress of moving IT systems into compliance with this policy. The analysis will identify, prioritize, and provide rationale for each production environment system as to its viability to move to the cloud within 2 to 5 years or not at all; and
 - (8) Authorize and maintain Mission-Area-specific FedRAMP commercial cloud provider ATOs, along with associated security control inheritance.

- k. System Owners in the Mission Areas, agencies, and staff offices will:
 - (1) Ensure through the Mission Area, Agency, and Staff Office Enterprise Architects that all existing and new cloud systems are registered in the USDA EAVE system;
 - (2) Ensure that statements of work, SLAs, and procurement requests for all cloud acquisition contracts include requirements for providing USDA with the proper level of performance and continuous accountability, availability, awareness, policy compliance, confidentiality, and integrity of the IT assets and data hosted on cloud services;
 - (3) Ensure adequate budgeting for operating, managing, and securing the cloud services as needed; and
 - (4) Document the configuration management and inventory management activities for cloud services.
- l. The Director of OHRM, who serves as the CHCO, will collaborate with the CIO and CFO to periodically update the training and hiring practices to ensure that the IT workforce has the skill sets needed to efficiently use cloud services.
- m. The CFO will:
 - (1) Annually, provide the Federal CIO with a written list of all cloud services that the Department has determined either cannot meet FedRAMP security authorization requirements or are not required to meet them according to the USDA CISO through the USDA Risk Management Framework. The USDA CIO and CFO must jointly sign this list; and
 - (2) Collaborate with the USDA CIO, the Director of OCP, and the CHCO to periodically update the procurement and acquisition practices to ensure that the Department has capital planning and talent acquisition strategies suitable for effective cloud adoption and services.
- n. The Director of OCP will:
 - (1) Ensure that all cloud contracts include cloud-appropriate acquisition language and SLAs to comply with Federal and Departmental regulations and policies; and
 - (2) Ensure that the General Counsel is engaged, when appropriate, for advice and counsel with respect to the acquisition and offering of cloud services.
- o. The Departmental Records Officer, within the Office of the General Counsel, Office of Information Affairs, will ensure that cloud service offerings comply with Federal and Departmental records management, eDiscovery, litigation hold, and National Archives

and Records Administration requirements, regulations, and policies. This includes compliance with the following USDA policies:

- (1) [DR 3080-001](#), *Records Management*;
 - (2) [DR 3085-001](#), *Vital Records Management Program*;
 - (3) [DR 3090-001](#), *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*; and
 - (4) [DR 3099-001](#), *Records Management Policy for Departing Employees, Contractors, Volunteers and Political Appointees*.
- p. The General Counsel will provide legal services, legal oversight advice, and counsel with respect to the acquisition and offering of cloud services and policy covered in this DR.
- q. Mission Area, Agency, and Staff Office Enterprise Architects will assist Mission Areas, agencies, and staff offices in registering and reporting all existing and new cloud systems and services to the USDA EAVE.

8. POLICY EXCEPTIONS

- a. All USDA Mission Areas, agencies, and staff offices must conform to this regulation. However, if a specific regulation requirement cannot be met as explicitly stated, Mission Areas, agencies, and staff offices may submit a waiver request. The waiver request must explain the reason for the request, identify compensating controls and actions that meet the intent of the regulation, and identify how the compensating controls and actions provide a similar or greater level of defense or compliance than the regulation requirement. Mission Areas, agencies, and staff offices will address all policy waiver request memoranda to the USDA OCIO DISC ACIO at usda-cloud-policy@usda.gov.
- b. Policy waiver requests will be reviewed by the DISC ACIO, the CISO, and the CTO. Each may provide recommendations to the USDA CIO for consideration. The CIO will make the final waiver approval decision.
- c. Waivers granted approval by the USDA CIO must be associated with a NIST control and 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.

9. INQUIRIES

Direct inquiries about this policy to the USDA OCIO DISC ACIO at usda-cloud-policy@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

AAR	Acquisition Approval Request
ACIO	Associate Chief Information Officer
ATO	Authorization to Operate
CDM	Continuous Diagnostics and Mitigation
CFO	Chief Financial Officer
CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
Cloud Smart	The Federal Cloud Computing Strategy
CONOPS	Concept of Operations
CPIC	Capital Planning and Investment Control
CPOC	Cybersecurity and Privacy Operations Center (OCIO component)
CSP	Cloud Service Provider
CSWP	Cybersecurity White Paper
CTO	Chief Technology Officer
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DISC	Digital Infrastructure Services Center (OCIO Component)
DNS	Domain Name System
DNSSEC	Domain Name System Security Extension
DR	Departmental Regulation
EAVE	Enterprise Architecture Vision Environment
E.O.	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
FY	Fiscal Year
GSA	General Services Administration
IP	Internet Protocol
IRMC	Information Resource Management Center (OCIO component)
ISCM	Information Security Continuous Monitoring
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCP	Office of Contracting and Procurement
OHRM	Office of Human Resource Management
OMB	Office of Management and Budget
PII	Personally Identifiable Information
P.L.	Public Law

POA&M	Plan of Action and Milestones
RBD	Risk Based Decision
SLA	Service Level Agreement
SOP	Standard Operating Procedure
SP	Special Publication
TBM	Technology Business Management
TIC	Trusted Internet Connection
TTS	Technology Transformation Service
U.S.C.	United States Code
USDA	United States Department of Agriculture
WCAG	Web Content Accessibility Guidelines

APPENDIX B

DEFINITIONS

Cloud Broker. An entity that manages the use, performance, and delivery of cloud services and negotiates relationships between cloud providers and cloud consumers. (Source: NIST [SP 500-292](#), *NIST Cloud Computing Reference Architecture*)

Cloud Carrier. An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers. (Source: NIST SP 500-292)

Cloud Computing. A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (Source: NIST SP 800-145)

Cloud Consumer. A person or organization that maintains a business relationship with and uses service from cloud providers. (Source: NIST SP 500-292)

Cloud Provider. A person, organization, or entity responsible for making a service available to cloud consumers. (Source: NIST SP 500-292)

Continuous Diagnostics and Mitigation (CDM). The Continuous Diagnostics and Mitigation 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: DHS [Continuous Diagnostics and Mitigation \(CDM\) Program](#))

Continuous Monitoring. Maintaining ongoing awareness to support organizational risk decisions. (Source: NIST [SP 800-137](#), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*)

Contractor Support. Contractor support encompasses on-site or off-site contractor technical or other support staff. (Source: M-24-04)

Domain Name System (DNS). DNS is a distributed computing system that enables access to Internet resources by user-friendly domain names rather than Internet Protocol (IP) addresses, by translating domain names to IP addresses and back. (Source: NIST [SP 800-81-2](#), *Secure Domain Name System (DNS) Deployment 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. § 91](#), *Government Corporations*.

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 Systems Standards*)

Federal Information Technology Acquisition Reform Act (FITARA). As of December 2014, FITARA is a historic law that represented the first major overhaul of Federal IT in almost 20 years. Since FITARA's enactment, OMB published guidance to Federal agencies to ensure that this law is applied consistently Governmentwide in a way that is both workable and effective. This guidance is now available as OMB M-15-14. FITARA does the following:

1. Enhances the authority of the CIO;
2. Enhances transparency and risk management in IT investments;
3. Requires savings through IT portfolio review;
4. Expands training and use of IT cadres;
5. Consolidates Federal data centers;
6. Maximizes the benefit of the Federal Strategic Sourcing Initiative; and
7. Expands Governmentwide software purchasing programs.

(Sources: CIO.gov [Federal Information Technology Acquisition Reform Act \(FITARA\)](#); FITARA)

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, E.O., directive, policy, or regulation. (Source: NIST FIPS PUB 199)

Information Resources. Information and related resources, such as personnel, equipment, funds, and IT. (Source: *Paperwork Reduction Act of 1995*, [44 U.S.C. § 3501, et seq.](#), *SUBCHAPTER I—FEDERAL INFORMATION POLICY*)

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 an agency-operated information system. 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:

1. Federal information is adequately protected;
2. Federal information is logically segregated from the contractor, state, or grantee corporate infrastructure; and
3. 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. (Source: OMB M-12-20)

Information Systems. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: *Paperwork Reduction Act*)

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 the 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:

1. Requires the use of such equipment; or
2. 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: *Clinger-Cohen Act of 1996*, [40 U.S.C. § 11101, et seq.](#), *Subtitle III—Information Technology Management*)

PortfolioStat. 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 to maximize the return on IT investments across the portfolio. (Source: CIO.gov 6.2 *PortfolioStat*)

Private Cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple cloud consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. (Source: NIST SP 800-145)

Service Provider. A service provider encompasses the typical outsourcing of system or network operations, telecommunication services, or other managed services (including those provided by another agency or subscribing to software services). (Source: OMB M-12-20)

TechStat. A face-to-face, evidence-based accountability review of an IT investment for Federal agencies. (Source: CIO.gov 6.3 *TechStat*)

Zero Trust Architecture. Provides a collection of concepts designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as contested. (Source: NIST CSWP 20)

APPENDIX C

AUTHORITIES AND REFERENCES

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

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

[5 U.S.C. § 104](#), *Independent Establishment*

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

[40 U.S.C. § 11331](#), *Responsibilities for Federal Information Systems Standards*

CIO.gov, [6.2 PortfolioStat](#) web page

CIO.gov, [6.3 TechStat](#) web page

CIO.gov [Federal Information Technology Acquisition Reform Act \(FITARA\)](#) web page

Clinger-Cohen Act of 1996, [40 U.S.C. § 11101, et seq.](#), *Subtitle III—Information Technology Management*

DHS, [Continuous Diagnostics and Mitigation \(CDM\) Program](#) website

DHS, [Continuous Diagnostics and Mitigation Program](#) document

[E.O. 14028](#), *Improving the Nation’s Cybersecurity*, May 12, 2021

FISMA, [44 U.S.C. § 3551, et seq.](#), *Subchapter II—Information Security*

FITARA, [P.L. 113-291, Title VIII, Subtitle D, Sections 831-837](#), December 19, 2014

GSA, FedRAMP, [Program Basics](#) web page

GSA, TTS Handbook, [Federal Information Technology Acquisition Reform Act \(FITARA\)](#) web page

NIST, [CSWP 20](#), *Planning for a Zero Trust Architecture: A Planning Guide for Federal Administrators*, May 6, 2022

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

NIST, [Glossary](#) website

NIST, [SP 500-291](#), Version 2, *NIST Cloud Computing Standards Roadmap*, July 2013

NIST, [SP 500-292](#), *NIST Cloud Computing Reference Architecture*, September 2011

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

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

NIST, [SP 800-60](#), Revision 1, *Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008

NIST, [SP 800-81-2](#), *Secure Domain Name System (DNS) Deployment Guide*, September 2013

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

NIST, [SP 800-145](#), *The NIST Definition of Cloud Computing*, September 2011 (errata as of April 27, 2012)

OMB, CIO Council, [The Application Rationalization Playbook](#), June 2019

OMB, [Cloud Smart](#) web site

OMB, [FY 2021 IT Budget - Capital Planning Guidance](#), June 27, 2019

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-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-24-04, Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements](#), December 4, 2023

Paperwork Reduction Act of 1995, [44 U.S.C. § 3501, et seq.](#), Subchapter I—Federal Information Policy

USDA, [DR 3080-001](#), *Records Management*, August 16, 2016

USDA, [DR 3085-001](#), *Vital Records Management Program*, August 19, 2011

USDA, [DR 3090-001](#), *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*, May 28, 2008

USDA, [DR 3099-001](#), *Records Management Policy for Departing Employees, Contractors, Volunteers and Political Appointees*, July 2, 2012

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

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 3160-001](#), *Licensed Information Technology (IT) Software*, May 16, 2019

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

USDA, [DR 3185-001](#), *Enterprise Architecture*, April 19, 2022

USDA, [DR 3185-002](#), *Enterprise Architecture IT Asset Definitions*, September 22, 2020

USDA, [DR 3185-003](#), *Enterprise Architecture IT Asset Data Element Requirements*, February 23, 2021

USDA, [DR 3300-025](#), *Secure Domain Name System*, March 18, 2016

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

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

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

USDA, [DR 3520-002](#), *Configuration Management*, July 17, 2019

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

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

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

USDA, [EAVE](#) website

USDA, [Information Technology Strategic Plan 2022-2026](#), June 2022

USDA, [RBD-SOP-3540-003B](#), Revision 1.6, *USDA Standard Operating Procedures on Risk-Based Decision Management*, September 2021

USDA, *Risk Management Framework 2.0*, [Impact-Level Prioritization](#) web page

USDA, [Risk Management Framework 2.0](#) website

W3C, Web Accessibility Initiative (WAI), [WCAG 2 Overview](#) website, March 7, 2024