

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

|  |                                     |
|--|-------------------------------------|
| <b>DEPARTMENTAL REGULATION</b>               | NUMBER:<br>DR 3180-001              |
| SUBJECT: Information Technology Standards    | DATE:<br>January 5, 2021            |
| OPI: Office of the Chief Information Officer | EXPIRATION DATE:<br>January 5, 2026 |

| <u>Section</u>                          | <u>Page</u> |
|---|-------------|
| 1. Purpose                              | 1           |
| 2. Special Instructions/Cancellations   | 2           |
| 3. Scope                                | 2           |
| 4. Background                           | 2           |
| 5. Policy                               | 3           |
| 6. Roles and Responsibilities           | 4           |
| 7. Policy Exceptions                    | 5           |
| 8. Inquiries                            | 6           |
| 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 standards for the acquisition, configuration, and administration of information technology within the United States Department of Agriculture (USDA).
- b. Application of the standards accompanying this regulation supports and implements the guidance issued by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and other Federal oversight entities; facilitates the uniform application of engineering and technical criteria, methods, processes, and practices when evaluating and procuring new technologies; ensuring new technologies align with USDA enterprise architecture business goals and processes; and meets the requirements of the following policy documents:

(1) OMB, Circular [A-130](#), *Management of Federal Information Resources*; and

- (2) OMB, Circular [A-119](#), *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*.
- c. The benefits of standardization to the department, mission areas, agencies, staff offices, and users are:
- (1) Provides cost savings and improved integration through elimination or consolidation of duplicative processes, systems, and technologies;
  - (2) Ensures acquisition and use of standard information technologies and cloud services
  - (3) Ensures correctness, completeness, and currency of the Standard Profiles through the definition of roles, responsibilities, and processes;
  - (4) Enhances interoperability between programs, systems, and services; and
  - (5) Improves consistency, accuracy, and timeliness of information shared across the USDA enterprise.

## 2. SPECIAL INSTRUCTIONS/CANCELLATIONS

This regulation supersedes DR 3180-001, *Information Technology Standards*, dated May 12, 2015.

## 3. SCOPE

This regulation applies to all USDA Mission Areas, agencies, staff offices, employees, and contractors working for or on behalf of USDA.

## 4. BACKGROUND

IT standards are rules or specifications designed to simplify, unify, or rationalize the design, interoperability, portability, and scalability of IT infrastructure components (e.g., network, hardware, systems, cloud services, and software).

The *Clinger-Cohen Act of 1996*, [40 United States Code \(U.S.C.\) § 11101](#), *et seq.*, (formerly known as the *Information Technology Management Reform Act (ITMRA)*), was enacted to improve the way the federal government acquires, uses and disposes of information technology (IT).

The *E-Government Act of 2002*, [Public Law \(P.L.\) 107-347](#), 116 Stat. 2899 (codified at various sections of title 44) drives the design and development of an enterprise architecture within Federal Agencies. OMB Circular A-130 requires that Federal agencies build and

maintain both a Profile of Standards and Technical Reference Model (TRM). The TRM has become the Application Reference Model (ARM) and Infrastructure Reference Model (IRM) in the *Federal Enterprise Architecture Framework (FEAF v2)* that support IT investment management and development of enterprise architecture.

OMB Circular A-119 requires Federal agencies to use voluntary consensus standards in lieu of government-unique standards, with the intention of reducing to a minimum the reliance by agencies on government-unique standards.

The [Common Approach to Federal Enterprise Architecture](#) presents an overall approach to developing and using Enterprise Architecture in the Federal Government by promoting increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies. Related implementation guidance from the OMB is contained in various documents, including Circular [A-11](#), *Preparation, Submission and Execution of the Budget*; Circular A-130; Memorandum [M-97-16](#), *Information Technology Architectures*; [M-00-10](#), *Procedures and Guidance on Implementing the Government Paperwork Elimination Act*; [M-05-22](#), *Transition Planning for Internet Protocol Version 6 (IPv6)*; [M-12-10](#), *Implementing PortfolioStat*; and the [Digital Government Strategy](#). The FEAF v2 is the suite of tools to help government planners implement the Common Approach.

## 5. POLICY

All USDA Mission Areas, agencies and staff offices must comply with the *E-Government Act of 2002*, OMB Circular A-130, OMB Circular A-119, and the FEAF v2, specifically the IRM artifact I-3 (Technical Standard Profile).

This regulation requires that all Mission Areas, agencies and staff offices under the administrative oversight of the USDA Office of the Chief Information Officer (OCIO) adhere to the [USDA Standards Profile Forecast](#) for systems, products, and applications. At a minimum, the USDA Standards Profile Forecast must be utilized when building out specific systems profiles. The other profiles attached to this directive must be utilized to identify specific and unique standards to each Mission Areas and their respective systems. All Mission Areas, agencies and staff offices must report to the USDA OCIO any deficiencies and provide status updates. The standards that are cited in the linked appendices will help Mission Areas, agencies and staff offices align their systems and applications to recognized, authoritative standards.

- a. Mission Areas, agencies, and staff offices will adhere to the following requirements when determining applicable standards for their respective systems:
  - (1) Establish uniform engineering and technical criteria;
  - (2) Establish methods, practices, and processes;

- (3) Align with NIST and *Federal Information Security Modernization Act of 2014* (FISMA), [44 U.S.C. § 3551](#), *et seq.*, security requirements;
- (4) Establishing net-centric and interoperable shared services throughout the agency and USDA;
- (5) Develop and establish technical maturity among systems and applications;
- (6) Ensure alignment of investments, systems, and applications to include infrastructure;
- (7) Manage the replacement of systems, applications, hardware, software, and other technologies that are in alignment with the current in force standards; and
- (8) Promote best practice alignment with business, performance, application, infrastructure, data and security configurations.

## 6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) will:
  - (1) Be the final approving authority on the adoption of all IT related standards for USDA infrastructure, with the goal of maximizing the benefit of technology purchases, and minimizing investment and operating expense; and
  - (2) Be the final reviewer and approver of exceptions to the IT standards when requested by the Mission Areas, agencies, and staff offices.
- b. The Information Resource Management Center (IRMC) Associate Chief Information Officer (ACIO) will:
  - (1) Develop policies, regulations, and requirements for the IT environment.
  - (2) Provide management and oversight activities related to business, performance, application, data, infrastructure, and security configurations, including but not limited to:
    - (a) Reviewing and monitoring compliance with established policy requirements and standards; and
    - (b) Reporting compliance and deviations to OMB.
- c. Mission Area Assistant CIOs will:
  - (1) Implement the policies, requirements, and standards for the IT environment by:

- (a) Developing internal procedures and controls in support of this regulation, as necessary;
  - (b) Establishing effective communication between internal stakeholders and OCIO; and
  - (c) Incorporating the policies, requirements, and standards into Mission Area capital planning and investment control (CPIC) processes.
- (2) Implement and maintain business, performance, application, data, infrastructure and security configuration settings by:
- (a) Documenting all deviations from standard configurations with a detailed rationale for the deviations, and request for a waiver from USDA ACIO OCIO-IRMC;
  - (b) Providing corrective action plans for the timely remediation of issues not authorized as an approved deviation;
  - (c) Consider the use of enterprisewide Blanket Purchase Agreements (BPA) when Procuring hardware, software, and IT services or GSA schedule contracts;
  - (d) Utilizing the Acquisition Approval Request (AAR) process, prior to any IT related procurements of \$25,000 or higher with the following consideration. The AAR must identify whether the acquisition of hardware, software or contractor support being procured meets the applicable standards, identifies the BPAs to be used, and provides a detailed rationale if the products and services being procured do not meet the applicable standards;
  - (e) Ensure adherence and compliance with NIST and (Federal Information Processing Standards) FIPS standards prior to utilizing ISO standards. NIST and FIPS standards should be used in preference to ISO standards. ISO standards would only apply if there are no applicable NIST or FIPS standards; and
  - (f) Use the EA tool, Enterprise Architecture Visioning Environment (EAVE) to build out their respective profiles and forecast or provide an API to their EA repositories to provide the link needed to build out their profiles.

## 7. POLICY EXCEPTIONS

All USDA Mission Areas, agencies, and staff offices are required to 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. Approved waivers

will be tracked as Plans of action and Milestones (POA&M) items. 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 must address all policy waiver request memoranda to the USDA ACIO-OCIO-IRMC and submit the request to the Enterprise Architecture Division for review and decision via email to [enterprise.architecture@usda.gov](mailto:enterprise.architecture@usda.gov).

Unless otherwise specified, Mission Areas, agencies, and staff offices will review and renew approved policy waivers every fiscal year. The ACIO OCIO-IRMC will monitor and approve waivers to this policy within 10 working days. If the ACIO OCIO-IRMC has not responded to the requesting Mission Area Assistant CIO or designee, the USDA OCIO will consider the waiver approved. The ACIO OCIO-IRMC will not disapprove waiver requests without documented consultation with, and concurrence from, the requesting Mission Area Assistant CIO or designee.

The written exception will be in the form of a decision memorandum and will include:

- a. Indication of Request for Exception;
- b. Name of submitting agency or staff office;
- c. Name and contact information of submitting person; and
- d. Information technology description (hardware and software exception):
- e. Justification to show good cause for the exception. The request should document the justifications for the exception; and
- f. The impact of granting versus not granting the request.

## 8. INQUIRIES

All USDA Mission Areas, agencies, and staff offices are to direct all questions and inquiries to the Office of the Chief Information Officer (OCIO), Information Resource Management Center (IRMC), EAD via email at [enterprise.architecture@usda.gov](mailto:enterprise.architecture@usda.gov).

-END-

## APPENDIX A

### ACRONYMS AND ABBREVIATIONS

|           |   |
|-----------|---|
| AAR       | Acquisition Approval Request  |
| ACIO      | Associate Chief Information Officer   |
| ARM       | Application Reference Model   |
| BPA       | Blanket Purchase Agreement  |
| CIO       | Chief Information Officer   |
| CPIC      | Capital Planning and Investment Control   |
| DDMS      | Department of Defense Discovery Metadata Specification (DoD Discovery Metadata Specification) |
| DoDAF     | Department of Defense Architecture Framework  |
| DR        | Departmental Regulation   |
| EAVE      | Enterprise Architecture Visioning Environment   |
| FEAF      | Federal Enterprise Architecture Framework   |
| FIPS      | Federal Information Processing Standards  |
| FISMA     | Federal Information Security Modernization Act  |
| IEC       | International Electrotechnical Commission   |
| IETF      | Internet Engineering Task Force   |
| IRM       | Infrastructure Reference Model  |
| ISO       | International Organization for Standardization  |
| IT        | Information Technology  |
| ITMRA     | Information Technology Management Reform Act  |
| JPEG      | Joint Photographic Experts Group  |
| MPEG      | Moving Picture Experts Group  |
| NCE       | Net-Centric Environment   |
| NIST      | National Institute of Standards and Technology  |
| NITF      | National Imagery Transmission Format  |
| OCIO      | Office of the Chief Information Officer   |
| OCIO-IRMC | Office Chief Information Officer-Information Resource Management Center                       |
| OMB       | Office of Management and Budget`  |
| OWL       | Web Ontology Language   |
| P.L.      | Public Law  |
| POA&M     | Plan Of Action and Milestones   |
| RFC       | Request for Comments  |
| TRM       | Technical Reference Model   |
| UCORE     | Universal Core  |
| U.S.C.    | United States Code  |
| USDA      | United States Department of Agriculture   |
| XML       | Extensible Markup Language  |

## APPENDIX B

### DEFINITIONS

Application Reference Model (ARM). The Application Reference Model (ARM) is the framework for categorizing Federal IT systems and application components to help identify opportunities for sharing, reuse, and consolidation or renegotiation of licenses. This information will often be used in conjunction with the other Reference Models to identify these opportunities. Application is defined as: Software components (including websites, databases, email, and other supporting software) resting on Infrastructure that, when aggregated and managed, may be used to create, use, share, and store data and information to enable support of a business function. The ARM is a categorization of different types of software, components and interfaces. It includes software that supports or may be customized to support business. It does not include operating systems or software that is used to operate hardware (firmware) because these are contained in the IRM. (Source: *Federal Enterprise Architecture Framework*, v 2.0)

Information Technology (IT). The term "information technology" means 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 an 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: OMB, Circular A-130 Revised, *Management of Federal Information Resources*)

Infrastructure Reference Model (IRM). The Infrastructure Reference Model (IRM) is the framework and taxonomy-based reference model for categorizing IT infrastructure and the facilities that host and contain the IT infrastructure. For the purposes of IRM, Infrastructure is defined as “The generic (underlying) platform consisting of hardware, software, and delivery platform upon which specific or customized capabilities (solutions, applications) can be deployed.” The purpose of the IRM is to provide the foundation for classifying the technology infrastructure and the physical infrastructure that is needed to support it. The IRM supports definition of infrastructure technology items and best practice guidance to promote positive outcomes across technology implementations. (Source: *Federal Enterprise Architecture Framework*, v 2.0)

IT Standards Profile/Technical Standards Profile. The IT Standards Profile collates the various systems and services, standards, and rules that implement and constrain the choices that can be or were made in the design and implementation of an Architectural Description. It delineates the systems, services, Standards, and rules that apply. The technical standards govern what hardware and software may be implemented and on what system. The standards that are cited may be international such as ISO standards, national standards, or organizational specific

standards. With associated standards with other elements of the architecture, a distinction is made between applicability and conformance. If a standard is applicable to a given architecture, that architecture need not be fully conformant with the standard. The degree of conformance to a given standard may be judged based on a risk assessment at each approval point. Note that an association between a Standard and an architectural element should not be interpreted as indicating that the element is fully compliant with that Standard. Further detail would be needed to confirm the level of compliance. Standards Profiles for a particular architecture must maintain full compatibility with the root standards they have been derived from. In addition, the IT Standards Profile model may state a method of implementation for a Standard, as compliance with a Standard does not ensure interoperability. The Standards cited are referenced as relationships to the systems, services, system functions, service functions, system data, service data, hardware and software items, or communication protocols. (Source: *The DoDAF Architecture Framework*, Version 2.02)

Net-Centric Environment (NCE). The Net-Centric Environment is a framework for full human and technical connectivity and interoperability that allows all users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence; and protects information from those who should not have it. (Source: *Net-Centric Environment Joint Functional Concept*, Version 1.0)

Standards Defined. The term “standard,” or “technical standard” as cited in National Technology Transfer and Advancement Act of 1995, includes all of the following: (1) common and repeated use of rules, conditions, guidelines, or characteristics for products or related processes and production methods; and related management systems practices; and (2) the definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength. A standard is a document, established by consensus that provides rules, guidelines or characteristics for activities or their results (as defined in ISO/IEC Guide 2:2004). It is a basis for comparison; a reference point against which other things can be evaluated. A standard is a formal document that establishes uniform engineering or technical criteria, methods, processes and practices. A standard is an exact value, a physical entity, or an abstract concept, established and defined by authority, custom, or common consent to serve as a reference, a model, or a rule in measuring quantities or qualities, establishing practices or procedures, or evaluating results. It is a fixed quantity or quality. A data standard is an established structured representation for data exchange. It is documented by a specification for an explicit set of requirements and may have associated eXtensible Markup Language (XML) artifacts (e.g., schema, OWL, schematron, stylesheet). Data standards containing one or more associated XML artifacts are designated technical data standards (e.g., JPEG, MPEG, NITF, DDMS, UCORE). Data standards not containing XML artifacts are designated abstract data standards (e.g., IETF RFC 3339, ISO Technical Committee 211, ISO 8601, ISO 3166). (Source: ISO/IEC Guide 2:2004, Standardization and related activities)

Technical Reference Model (TRM). The Technical Reference Model (TRM) is a component-driven, technical framework categorizing the standards and technologies to support and enable the delivery of Service Components and capabilities. The TRM has been split into the ARM and

IRM as defined above by the release of FEAF v2. (Source: *Federal Enterprise Architecture Framework*, v 2.0)

## APPENDIX C

### AUTHORITIES AND REFERENCES

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

[Common Approach to Federal Enterprise Architecture](#), May 2, 2012

Department of Defense, [The DoDAF Architecture Framework](#), Version 2.02, August 2010

[Digital Government: Building a 21st Century Platform to Better Serve The American People](#), May 23, 2012

*E-Government Act of 2002*, [P.L. 107-347](#), 116 Stat. 2899, December 17, 2002

*Federal Information Security Modernization Act of 2014 (FISMA)*, [44 U.S.C. § 3551](#), *et seq.*, December 8, 2014

[Internet Engineering Task Force/Request for Change \(IETF/RFC\) 3339](#), *Date and Time on the Internet: Timestamps*, July 2002

[International Organization for Standardization \(ISO\) 3166](#), *Codes for the Representation of Names of Countries and their Subdivisions*

[ISO 8601:2004](#), *Data Elements and Interchange Formats -- Information Interchange -- Representation of Dates and Times*

[ISO/IEC Guide 2:2004](#), *Standardization and related activities -- General vocabulary*

[ISO Technical Committee 211](#), *Geographic Information/Geomatics*

*National Technology Transfer and Advancement Act of 1995*; [P.L. 104-113](#), 110 Stat. 775, March 7, 1996 (codified in various sections of 15 U.S.C)

[Net-Centric Environment Joint Functional Concept](#), Version 1.0, October 31, 2005

OMB, Circular [A-11](#), *Preparation, Submission, and Execution Of The Budget*, July 2013

OMB, Circular [A-119](#), Revised, *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, February 10, 1998

OMB, Circular [A-130](#), Revised, *Management of Federal Information Resources*, February 8, 1996

OMB, *Federal Enterprise Architecture Framework*, v 2.0 ([FEAF v 2.0](#)), January 29, 2013

OMB, Memorandum [M-97-16](#), *Information Technology Architectures*, June 18, 1997

OMB, Memorandum [M-00-10](#), *OMB Procedures and Guidance on Implementing the Government*, April 25, 2000

OMB, Memorandum [M-05-22](#), *Transition Planning for Internet Protocol Version 6 (IPv6)*, August 2, 2005

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

USDA, [DR 0100-001](#), *Departmental Directives System*, January 4, 2018

USDA, [USDA Standards Profile](#) web page