

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

<b>DEPARTMENTAL REGULATION</b>	NUMBER: DR 3180-001
SUBJECT: Information Technology Standards	DATE: May 12, 2015
	OPI: Office of the Chief Information Officer

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

## 1. PURPOSE

This Departmental Regulation (DR) establishes the baseline standards for the acquisition, configuration, and administration of information technology within the United States Department of Agriculture (USDA).

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/or technical criteria, methods, processes, and practices when evaluating and procuring new technologies; ensures new technologies align with USDA enterprise architecture business goals and processes; and meets the requirements of the following policy documents:

- a. OMB, [Circular A-130](#), *Management of Federal Information Resources*; and
- b. [OMB Circular A-119](#), *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*.

The benefits of standardization to the Department, agencies, staff offices, and users are:

- c. Provide cost savings and improved integration through elimination or consolidation of duplicative processes, systems, and/or technologies;
- d. Ensures acquisition and use of standard information technologies and/or cloud services
- e. Ensures correctness, completeness, and currency of the Standard Profiles through the definition of roles, responsibilities, and processes
- f. Enhance interoperability between programs, systems, and services; and
- g. Improve consistency, accuracy, and timeliness of information shared across the USDA enterprise.

## 2. SCOPE

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

## 3. SPECIAL INSTRUCTIONS/CANCELLATIONS

This regulation supersedes DR 3180-001, *Information Technology Network Standards*, dated September 30, 2008.

## 4. BACKGROUND

The [Clinger-Cohen Act of 1996](#) 40 U.S.C. §11101 et seq. (2014) (formerly known as the *Information Technology Management Reform Act* (ITMRA)), was enacted to improve the way the federal government acquires, uses and disposes information technology (IT). The [E-Government Act of 2002](#) P.L. 107-347, 116 Stat. 2899 (2002) (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.

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 [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 Circulars [A-11](#), A-130,

Memoranda [97-16](#), [00-10](#), [05-22](#), [11-29](#), [12-10](#), 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 agencies and staff offices shall comply with *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 agencies and staff offices under the administrative oversight of the USDA Office of the Chief Information Officer (OCIO) adhere to the USDA Standards Profile for systems/products and applications. At a minimum, the Mandatory USDA Baseline Standards Profile must be utilized when building out specific systems profiles. The other profiles attached to this directive shall be utilized to identify specific and unique standards to each agency and their respective systems. All agencies and staff offices shall report to the USDA OCIO any deficiencies and provide status updates. The standards that are cited in the linked appendices will help agencies and staff offices align their systems and applications to recognized, authoritative standards.

- a. Agencies and staff offices shall 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 Management Act ("[FISMA](#)"), 44 U.S.C. § 3541, et seq.(2014) 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.

- b. Agencies and staff offices shall operate network infrastructure, communications, applications, interfaces, security, data centers, and facilities consistent with the standards that are identified in the accompanying appendices.
- c. The following appendices can be accessed via hyperlink on a USDA Connection site. These profiles are located under the “Files” section. User will need to click on the “Folders” tab and then click on the folder named “Baseline Standards Profiles;” the site requires permission to access, send requests to [enterprise.architecture@ocio.usda.gov](mailto:enterprise.architecture@ocio.usda.gov):
  - (1) [USDA Baseline Standards Profile – Mandatory](#)
  - (2) [USDA Baseline Standards Profile – Application Services](#)
  - (3) [USDA Baseline Standards Profile – Data & Databases](#)
  - (4) [USDA Baseline Standards Profile – Geospatial](#)
  - (5) [USDA Baseline Standards Profile – Infrastructure Services](#)
  - (6) [USDA Baseline Standards Profile – Interoperability](#)
  - (7) [USDA Baseline Standards Profile – Security Services](#)
  - (8) [USDA Baseline Standards Profile – Technical Support](#)
  - (9) [USDA Baseline Standards Profile – User Portals](#)

## 6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) shall:
  - (1) Be the final approving authority on the adoption of all IT related standards for USDA networks, 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 agencies or staff offices.
- b. The Associate Chief Information Officer (ACIO), Information Resource Management (IRM) shall:
  - (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. Agency and Staff Office CIOs shall:

- (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 agencies and staff office 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-IRM;
  - (b) Providing corrective action plans for the timely remediation of issues not authorized as an approved deviation;
  - (c) Utilizing the approved [USDA products list](#), located in the Baseline Standards Profile folder as noted in paragraph 5c, as developed by the Standards Technical Working Group (STWG), to procure products that are aligned to the applicable baseline standards (i.e., the Common Criteria standard [International Organization for Standardization \(ISO\)/International Electrotechnical Commission \(IEC\), 15408 – 1:2009](#));
  - (d) Employing the use of the [NIST Security Content Automation Protocol \(SCAP\)](#) compliant tool(s) to help evaluate providers and perform self-evaluations;
  - (e) Consider the use of enterprise-wide Blanket Purchase Agreements (BPAs) when Procuring hardware, software, and IT services or GSA schedule contracts;
  - (f) Utilizing the [Acquisition Approval Request \(AAR\) process](#) , located in the Baseline Standards Profile folder as noted in 5c, prior to any IT related procurements of \$25,000 or higher with the following exception. The AAR must identify whether or not 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 product(s) and services being procured do not meet the applicable standards; and

- (g) Ensure adherence/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.

## 7. POLICY EXCEPTIONS

All USDA agencies and staff offices are required to conform to this regulation; however, in the event that a specific regulation requirement cannot be met as explicitly stated, agencies/staff offices may submit a waiver request. The waiver request shall explain the reason for the request, identify compensating controls/actions that meet the intent of the regulation, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the regulation requirement. Agencies and staff offices shall address all policy waiver request memoranda to the USDA ACIO-OCIO-IRM and submit the request to the Enterprise Architecture Division for review and decision via email to [enterprise.architecture@ocio.usda.gov](mailto:enterprise.architecture@ocio.usda.gov).

Unless otherwise specified, agencies and staff offices shall review and renew approved policy waivers every fiscal year. Approved waivers shall be tracked as a plan of action and milestones (POA&M) item. The ACIO OCIO-IRM shall monitor and approve waivers to this policy within 10 working days. If the ACIO OCIO-IRM has not responded to the requesting Agency CIO or designee, the USDA OCIO shall consider the waiver approved. The ACIO OCIO-IRM shall not disapprove waiver requests without documented consultation with, and concurrence from, the requesting Agency 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/software exception):
  - (1) Justification to show good cause for the exception. The request should document the justifications for the exception; and
  - (2) The impact of granting versus not granting the request.

-END-

## APPENDIX A

### REFERENCES

[Circular No. A-11](#), *Preparation, Submission, and Execution Of The Budget*, July 2013

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

[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 (2002)

Federal Information Security Management Act of 2002 ("[FISMA](#)"), 44 U.S.C. § 3541, et seq.(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/IEC 15408-1:2009, *Information technology — Security techniques — Evaluation criteria for IT security - Part 1: Introduction and general model Common Criteria) Third Edition*, December 15, 2009

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

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

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

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

[M-11-29](#), Chief Information Officer Authorities, August 8, 2011

[M-12-10](#), Implementing Portfolio Stat, March 30, 2012

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

[NIST Security Content Automation Protocol \(S-CAP\)](#), May 12, 2009

Office of Management and Budget (OMB), *Federal Enterprise Architecture Framework, v 2.0* ([FEAF v 2.0](#)), January 29, 2013

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

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

[The Clinger-Cohen Act of 1996](#), 40 U.S.C. §11101 et seq. (2014)  
*USDA Enterprise Roadmap 2014*, March 28, 2014

## APPENDIX B

### 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)
DR	Departmental Regulation
FEAF	Federal Enterprise Architecture Framework
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IRM	Infrastructure Reference Model
ISO	International Organization for Standardization
ITMRA	Information Technology Management Reform Act
IT	Information Technology
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
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
SCAP	Security Content Automation Protocol
STWG	Standards Technical Working Group
OCIO-IRM	Office Chief Information Officer-Information Resource Management
TRM	Technical Reference Model
UCORE	Universal Core
USDA	United States Department of Agriculture
XML	Extensible Markup Language

## APPENDIX C

### DEFINITIONS

#### Application Reference Model

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 Web sites, 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 (e.g., firmware) because these are contained in the IRM.

#### Infrastructure Reference Model

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/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.

#### Information Technology

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 (i) requires the use of such equipment, or (ii) 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.

### 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.

### Technical Reference Model

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.

### 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 particular 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/software items, or communication protocols.

### 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; (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).