

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

DEPARTMENTAL MANUAL	NUMBER: DM 3180-001
SUBJECT: Information Technology Standards Procedures	DATE: July 29, 2019
OPI: Office of the Chief Information Officer, Information Resource Management Center (IRMC)	EXPIRATION DATE: July 29, 2024

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Scope	2
3. Special Instructions/Cancellations	2
4. Background	2
5. Requirements, Profiles, and Forecasts	4
6. Procedures	6
7. Roles and Responsibilities	9
8. Inquiries	10
Appendix A – Acronyms and Abbreviations	A-1
Appendix B – Authorities and References	B-1

1. PURPOSE

- a. This Departmental Manual (DM) establishes the processes required for determining which standards (technical, data, and hybrid (technical/data)) to use for the acquisition, configuration, and administration of information technology (IT) within the United States Department of Agriculture (USDA).
- b. This DM provides the procedures necessary to apply Departmental Regulation (DR) [DR 3180-001](#), *Information Technology Standards*, throughout USDA. DR 3180-001 supports and implements the guidance issued by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), the *Federal Information Technology Acquisition Reform Act* (FITARA), [Public Law \(P.L.\) 113-291 Sections 831-837](#), and other Federal oversight entities. It 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 (EA), business goals, and processes; and meets the requirements of the following policy documents:

- (1) OMB, Circular [A-130](#), *Managing Information as a Strategic Resource*; 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 all users within USDA include:
- (1) Providing cost avoidance and improved integration through elimination or consolidation of duplicative processes, systems, and/or technologies;
 - (2) Ensuring acquisition and use of standard information technologies and/or cloud services;
 - (3) Ensuring correctness, completeness, and currency of the standard profiles through the definition of roles, responsibilities, and processes;
 - (4) Enhancing interoperability (data, security, technology) between programs, systems, and services; and
 - (5) Improving consistency, accuracy, and timeliness of information shared across the USDA enterprise.

2. SCOPE

This DM supports DR 3180-001 and applies to all USDA Mission Areas, agencies, staff offices, employees, and contractors working for, or on behalf of, USDA.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. Use this DM in conjunction with DR 3180-001.
- b. The term “agency” or phrase “agency and staff office,” unless otherwise noted in this document, will be considered to encompass the Mission Areas, agencies, and staff offices of USDA.

4. BACKGROUND

The *Clinger-Cohen Act of 1996*, [40 United States Code \(U.S.C.\) Section 11101](#) et seq. (2017) was enacted to improve the way the Federal Government acquires, uses, and disposes of IT. The *E-Government Act of 2002*, [Public Law \(P.L.\) 107-347](#) (codified at various sections of Title 44, Chapters 35 and 36) drives the design and development of an EA within Federal Agencies.

Circular A-119 requires Federal Agencies to use voluntary consensus standards in lieu of unique Government standards, with the intention of reducing to a minimum the reliance by Agencies on unique Government standards. The following are examples of voluntary consensus standards bodies: International Organization for Standardization (ISO), Federal Geographic Data Committee (FGDC), National Information Exchange Model (NIEM), and World Wide Web Consortium (W3C).

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).

FITARA requires that the Department's Chief Information Officer (CIO) coordinate FITARA-related activities with other senior Department officials including: the Chief Financial Officer (CFO), the Chief Acquisition Officer (CAO), the Chief Operating Officer (COO), the Deputy Secretary, represented by the USDA Assistant Secretary for Administration, the Senior Procurement Executive (SPE), the Chief Human Capital Officer (CHCO), and the Director of the Office of Budget and Program Analysis (OBPA). The USDA CIO, CFO, COO, CAO, SPE, CHCO, and OBPA Director, as a group, identify as the Chief Executive Officers (CXO). The CXOs tasks include fully defining and understanding the costs of Mission Area, agency, and staff office IT investments, products, and services be incorporated into the USDA budget formulation, budget execution, acquisition, and IT workforce-planning processes.

[DR 3185-001](#), *Enterprise Architecture*, states, "A documented and understood EA provides a framework for the organization to respond quickly to changes in its operating environment. It serves as a ready reference that enables the organization to assess the impact of the changes on each of the six EA components (business, data, infrastructure, technology, applications, and security), as well as ensuring the components continue to operate smoothly through the changes." The Technical Standards Profile is part of the Infrastructure domain.

[The Common Approach to Federal Enterprise Architecture](#) (*Common Approach*) presents an overall approach to developing and using EA in the Federal Government by promoting increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies. Within the *Common Approach*, in the Infrastructure Domain, the I-3, Technical Standards Profile is the artifact that captures the relevant standards that are in support of the systems that the Mission Area, agency, or staff office maintains. Related implementation guidance from the OMB is contained in various documents, including Circulars [A-11](#), *Preparation, Submission, and Execution of the Budget*; A-130; OMB, Memoranda [M-00-10](#), *OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act*; [M-05-22](#), *Transition Planning for Internet Protocol Version 6 (IPv6)*; [M-11-29](#), *Chief Information Officer Authorities*; [M-12-10](#), *Implementing PortfolioStat*; and the [Digital Government: Building a 21st Century Platform to Better Serve The American People](#). The *Federal Enterprise Architecture Framework, v 2.0 (FEAF v2)* is the suite of tools to help Government planners implement the *Common Approach*.

5. REQUIREMENTS, PROFILES, AND FORECASTS

a. Requirements

- (1) Identification of standards for systems relies on the business, functional, and technical requirements of the system as determined by the system owners/stakeholders. Business, functional, and technical requirements will help to identify standards for a system.
- (2) Business requirements, which are not technical in nature, focus on fulfilling Mission Area, agency, and staff office needs or business goals. Functional requirements are technical and provide detailed information about how a software system functions. Business requirements for a project are a series of needs that achieve a high-level objective.
- (3) Business requirements describe the customers' needs. They clearly state Mission Area, agency, and staff office objectives and prioritize the problems Mission Areas, agencies, and staff offices need to solve. These documents do more than just narrate the needs and solutions. They may contain diagrams, organizational charts, and flowcharts.
- (4) Functional requirements describe how a software system functions. They delve into how users interact with the software, such as what actions occur after users click on buttons and show the outcome of these actions. Functional requirements also show how other databases or software applications integrate with each other. They specify the hardware and operating system requirements that the software system will be using. Functional requirements are a detailed breakdown that explains how the outcome of a project will operate to meet the specified business requirements that address a specific need or pain point identified by the end user or stakeholder.
- (5) Technical requirements establish what a Mission Area, agency, or staff office needs to do to support the project's outcome during and after implementation.

The standards profile defines the technical, operational, business, policy, and guidance standards applicable to the architecture. In addition to identifying applicable technical standards, the standards profile also documents the policies and standards that apply to the operational or business context.

b. Profiles

- (1) In most cases, building a standards profile consists of identifying and listing the applicable portions of existing and emerging documentation. A Standards Profile should identify both existing guidelines, as well as any areas lacking guidance. As with other models, each profile is assigned a specific timescale (e.g., as-is, to-be, or transitional). Linking the profile to a defined timescale enables the enterprise architect to consider both emerging technologies and any current technical

standards that are being updated (becoming mature) or becoming obsolete (to be retired).

- (2) The standards profile collates and delineates the various systems and services, standards, and rules that implement and constrain the choices in the design and implementation of an architectural description. The technical standards govern what hardware and software may be implemented and on what system. The standards cited may be international (such as ISO standards), national standards, or organizational specific standards.
- (3) With associated standards, as with other elements of the architecture, a distinction between applicability and conformance. If a standard is applicable to a given architecture, that architecture need not fully conform with the standard. The degree of conformance to a given standard is based on a risk assessment at each approval point.

Note that an association between a standard and an architectural element does not indicate that the element is fully compliant with that standard; rather further detail would need to confirm the level of compliance.

- (4) Standards profiles for an architectural design must maintain full compatibility with the root standards. Furthermore, the standards profile model may state a method of implementation for a standard, as compliance with a standard does not ensure interoperability.

c. Forecasts

The standards forecast contains expected changes in technical, operational, business, guidance, and policy standards and conventions documented in the standards profile.

- (1) A standards forecast is a detailed description of emerging standards relevant to the systems, operational, and business activities covered by the Architectural Description. The forecast focuses on areas that relate to the purpose for which a given architectural description should identify issues that affect the architecture. A standards forecast complements and expands on the standards profile and should be used when more than one emerging standard period is applicable to the architecture.
- (2) One of the prime purposes of a standards forecast is to identify critical technology standards, their fragility, and the impact of these standards on the future development and maintainability of the architecture and its constituent elements.
- (3) The standards forecast contains expected changes in standards and conventions, documented in the standards profile. One of the prime purposes of a standards forecast is to identify critical standards, their life expectancy, and the impact of these standards on the future development and maintainability of the architectural description and its constituent elements.

A Standards forecast lists emerging or evolving standards relevant to the solutions covered by the architectural description.

- (4) Ensure that the specific periods selected (e.g., 6-month, 18-month, 36-month intervals) and the standards being tracked are coordinated with architecture transition plans. That is, inserting new capabilities and upgrading existing solutions may depend on the availability of new standards and models incorporating those standards. The forecast specifies potential standards, thus influences current architectures and influences the development of transition and objective (i.e., target) architectures. The forecast focuses on standards/service areas that relate to the purpose for which a given architecture design described and should identify potential standards affecting that architecture.
- (5) The standards forecast delineates the standards that potentially affect the relevant system and service elements and relates them to the periods. A system's evolution, or service's evolutions, ties to a future standard listed in the standards forecast. A timed technology and skills forecast relates to the standards forecast in the following manner: a certain technology may depend on a standards forecast standard (i.e., a standard listed in the standards forecast may not be adopted until a certain technology becomes available). This is how a prediction on the adoption of a future standard may be related to standards listed in the standards profile.

6. PROCEDURES

- a. Mission Area, agency, and staff office Enterprise Architects shall adhere to the following procedures when determining relevant standards for their respective systems profiles and forecasts:
 - (1) Establish uniform engineering and technical criteria;
 - (2) Establish methods, practices, and processes;
 - (3) Align with NIST and the *Federal Information Security Modernization Act of 2014* (FISMA), [44 U.S.C. 3551](#), et seq., security requirements;
 - (4) Establish net-centric and interoperably-shared services throughout the Mission Areas, agencies and staff offices throughout USDA;
 - (5) Develop and establish technical maturity among systems and applications;
 - (6) Ensure alignment of investments, systems, and applications to include infrastructure;

- (7) The use of open standards, which means widely accepted and supported standards set by recognized standards organizations or the marketplace. The standards should support interoperability, portability, and scalability and be equally available;
 - (8) Manage the replacement of systems, applications, hardware, software, and other technologies that are in alignment with the current in-force standards; and
 - (9) Promote best practices regarding alignment with business, performance, application, infrastructure, data, and security configurations.
- b. Construct technical system standards profiles and forecasts using the following procedure/steps:
- (1) Determine the specific need or pain point based on requirements that need to be addressed:
 - (a) Systems do not exist that could address the needs of the stakeholder.
 - (b) Are there current systems not meeting needs of the customer/stakeholder?
 - (c) The customer/stakeholder identifies requirements that a Mission Area, agency, or staff office needs to ensure mission completeness.
 - (2) Identify business, functional, and technical requirements for system(s) to address the need/pain point experienced by the stakeholder/customer:
 - (a) Determine the business, functional, and technical requirements that currently exist or need to be developed.
 - (b) Identify and capture requirements based on information gathering with the stakeholders.
 - (c) Discuss with the development staff the requirements obtained from the stakeholder and determine if a current system needs enhancement or if a new system needs development.
 - (3) Determine if there is an existing, approved capability that will satisfy the new requirements:
 - (a) Is there a known shared service that can be used to address the need/pain point identified by another Mission Area, agency, or staff office?
 - (b) Will the identified system interoperate with the current Mission Area, agency, or staff office's system or application?
 - (c) Is there an existing standards profile/forecast?

(d) Provide standards profile/forecast to shared site.

1 Profiles/forecasts should reflect ability to address the current system or application requirements.

2 Profiles/forecasts should also incorporate identified requirements.

(4) If no system/shared service exists:

(a) Consult with the Enterprise Architecture Division (EAD) to determine if there is an approved platform standard for the business need.

(b) If not, conduct an analysis of alternatives (AOA) and identify recommended solution (s) (to include systems and subsystems); and

(c) Use identified requirements to:

1 Identify standards to address system requirements to operate within the Mission Area, agency, and staff office environment; and

2 Use a standards forecast to identify the future state once a commercial off-the-shelf (COTS) or Government off-the-shelf (GOTS) product is identified.

(5) A Determination needs to be made:

(a) Is the product a COTS or customized GOTS system/subsystem?

(b) If COTS, ensure that the vendor is compliant with a baseline standards profile, identified in DR 3180-001, to operate within the Mission Area, agency, and staff office network; and

(c) If GOTS, ensure that the development staff works with the entities that can identify current and in-force standards as identified in DR 3180-001.

(6) Are the products COTS products that make up the system/subsystem on the Common Criteria [*Certified Products List*](#)?

(a) Are the COTS products certified to standard International Standards Organization/International Electrotechnical Commission [*ISO/IEC 15408-1:2009, Information technology — Security techniques — Evaluation criteria for IT security - Part 1: Introduction and general model Common Criteria*](#))?

- (b) If not, an alternative/approved product will need researching, or a waiver with risk mitigation plan and strategy needs submission for consideration to the OCIO, Information Resource Management Center (IRMC), EAD.
- (7) Determine service areas (web services, network, security, etc.):
- (a) Is the system providing email services?
 - (b) Is it a shared service (interoperability)?
 - (c) Is it using cloud or providing cloud services?
- (8) Identify standards:
- (a) When identifying standards keep in mind they can cover more than one service area.
 - (b) Does the baseline standards profile or forecast contain the standards as noted in DR 3180-001?
 - (c) If not listed in the DR 3180-001 profiles:
 - 1 Consult with the Standards Architect to determine if adding to profile or forecast or need for more research; and
 - 2 Determination of which product (profile or forecast) is based on age of the standard and use of the standard in user community (other government or private entities).
- (9) Build standards profiles/forecasts:
- (a) List the standards and service area(s) needed for system procurement or build based on requirements; and
 - (b) Provide profiles and forecasts with portfolio review packages.

7. ROLES AND RESPONSIBILITIES

- a. The USDA CIO will address the responsibilities as delineated in DR 3180-001, Section 6a.
- b. The Associate Chief Information Officer (ACIO), IRMC will address the responsibilities as delineated in DR 3180-001, Section 6b:

- c. The USDA Enterprise Architecture Committee (EAC) will:
 - (1) Collaborate with Mission Areas, agencies, and staff offices in the creation, maintenance, and updating of enterprise architecture standards, guidelines, directives and policies within USDA;
 - (2) Establish EA value and performance measures;
 - (3) Assess compliance with, completeness of, and benefits derived directly and indirectly from the use of the USDA EA standards; and
 - (4) Develop and maintain a standards profile and forecast for the USDA EA standards domain, and make recommendations to the USDA's CIO Council for improvements to USDA's EA standards domain.

- d. Mission Area, Agency, and Staff Office Enterprise Architects will:
 - (1) Implement the policies, requirements, and standards for the IT environment;
 - (2) Develop internal procedures and controls in support of this DM as necessary;
 - (3) Establish effective communication between internal stakeholders and IRMC leadership; and
 - (4) Incorporate the policies, requirements, and standards into Mission Area, agency, and staff office capital planning and investment control (CPIC) processes.

8. INQUIRIES

All USDA Mission Areas, agencies, and staff offices are to direct all questions and inquiries to the OCIO, IRMC, EAD via email at enterprise.architecture@ocio.usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

ACIO	Associate Chief Information Officer
AOA	Analysis of Alternatives
CAO	Chief Acquisition Officer
CFO	Chief Financial Officer
CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
COTS	Commercial Off-The-Shelf
CPIC	Capital Planning and Investment Control
CXO	Senior Agency Official such as a CAO, CFO, CHCO, CIO, COO
DAU	Defense Acquisition University
DM	Departmental Manual
DR	Departmental Regulation
EA	Enterprise Architecture
EAC	Enterprise Architecture Committee
EAD	Enterprise Architecture Division
FEAF	Federal Enterprise Architecture Framework
FGDC	Federal Geographic Data Committee
FISMA	Federal Information Security Modernization Act
FITARA	Federal Information Technology Acquisition Reform Act
GOTS	Government Off-The-Shelf
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IPT	Integrated Project Team
IPv6	Internet Protocol version 6
IRMC	Information Resource Management Center
ISO	International Organization for Standardization
IT	Information Technology
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
OBPA	Office of Budget and Program Analysis
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
P.L.	Public Law
RFC	Request for Comments
SCAP	Security Content Automation Protocol
SP	Special Publication
SPE	Senior Procurement Executive
U.S.C.	United States Code
USDA	United States Department of Agriculture
W3C	World Wide Web Consortium

APPENDIX B

AUTHORITIES AND REFERENCES

The *Clinger-Cohen Act of 1996*, [40 U.S.C. 11101](#) et seq., February 10, 1996 (2017)

Common Criteria, [Certified Products List](#)

Defense Acquisition University (DAU), [Glossary of Defense Acquisition Acronyms and Terms](#), 16th Edition, September 2015

[DR 3180-001](#), *Information Technology Standards*, May 12, 2015

[DR 3185-001](#), *Enterprise Architecture*, June 28, 2016

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

Federal Information Security Modernization Act of 2014 (FISMA), [44 U.S.C. 3551](#), et seq., December 18, (2017)

Federal Information Technology Acquisition Reform Act (FITARA), [Public Law \(P.L.\) 113-291, Title VIII, Subtitle D, Sections 831-837](#), December 19, 2014

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

ISO [3166](#), *Codes for the Representation of Names of Countries and their Subdivisions*, November 2013

ISO [8601](#):2004, *Data elements and interchange formats -- Information interchange -- Representation of dates and times*, December 2004

[ISO/IEC Guide 2:2004](#), *Standardization and related activities – General vocabulary*, November 2004 This standard was last reviewed and confirmed in 2016, therefore this version remains current

[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 This standard was last reviewed and confirmed in 2015, therefore this version remains current

NIST, [Security Content Automation Protocol \(SCAP\)](#), May 12, 2009

NIST, Special Publication [\(SP\) 800-128](#), *Guide for Security-Focused Configuration Management of Information Systems*, August 2011

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

OMB, [Circular A-11](#), *Preparation, Submission, and Execution of the Budget*, June 29, 2018

OMB, [Circular A-119](#), *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, January 27, 2016

OMB, [Circular A-130](#), *Managing Information as a Strategic Resource*, July 28, 2016

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

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

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

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

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

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

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

Definitions, [44 U.S.C. 3502](#) (2017)