

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

DEPARTMENTAL REGULATION	NUMBER: DR 3170-001
SUBJECT: End User Workstation Configurations	DATE: October 13, 2022
OPI: Office of the Chief Information Officer, Client Experience Center	EXPIRATION DATE: October 13, 2027

<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	4
7. Policy Exceptions	6
8. Inquiries	7
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 approved workstations and associated peripheral configurations for all users within the United States Department of Agriculture (USDA). Using permitted workstation configurations ensures and promotes greater cyber protection, compatibility, and interoperability for hardware and software and provides consistency and standardization for the acquisition, configuration, and administration of information technology (IT).
- b. Using acceptable workstation configurations supports and implements guidance issued by the Office of Management and Budget (OMB), National Institute of Standards and Technology (NIST), and other Federal oversight entities. Doing so facilitates the uniform application of engineering, technical criteria, methods, processes, and practices when evaluating and procuring new technologies; ensures that technologies align with USDA enterprise architecture business goals and processes; and meets the requirements of:

- (1) OMB, Circular [A-130](#), *Managing Information as a Strategic Resource*; and
- (2) [DR 3180-001](#), *Information Technology Standards*.

2. SCOPE

- a. This policy applies to all USDA Mission Areas, agencies, staff offices, employees, and contractors working for, or on behalf of, USDA.
- b. This DR does not apply to lab workstations or lab equipment.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This regulation supersedes DR 3170-001, *End User Workstation Configurations*, dated January 11, 2021.
- b. In this document, workstations are defined as desktop computers, mobile devices (laptop computers, mobile phones or tablets), and other computers and devices accessing the USDA network.

4. BACKGROUND

- a. Congressional mandates for IT architecture are contained in the *Clinger-Cohen Act of 1996*, [40 United States Code \(U.S.C.\) § 11101 et seq.](#), updated and revised by the *E-Government Act of 2002*, [44 U.S.C. § 3601](#), to help each Government agency build enterprise architecture.
- b. OMB, Circular [A-119](#), *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities*, requires that Federal agencies use voluntary consensus standards to reduce the reliance of Federal agencies' use of unique Government standards. Refer to DR 3180-001 for the definition of standards.
- c. [The Common Approach to Federal Enterprise Architecture](#) presents an overall approach to developing and using enterprise architecture in the Federal Government by promoting increased mission effectiveness through the standardization of the development and use of architectures within, and between, Federal agencies. Related implementation guidance from OMB is contained in various documents, including:
 - (1) OMB, Circular [A-11](#), *Preparation, Submission, and Execution of the Budget*;
 - (2) OMB, Circular [A-130](#), *Managing Information as a Strategic Resource*;

- (3) OMB, [M-00-10](#), *OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act*;
 - (4) OMB, [M-05-22](#), *Transition Planning for Internet Protocol Version 6 (IPv6)*;
 - (5) OMB, [M-11-29](#), *Chief Information Officer Authorities*;
 - (6) OMB, [M-12-10](#), *Implementing PortfolioStat*;
 - (7) OMB, Memorandum [M-17-26](#), *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*; and
 - (8) [Digital Government: Building a 21st Century Platform to Better Serve the American People](#).
- d. The [Federal Enterprise Architecture Framework, Version 2](#) (FEAF v2), is a suite of tools to help Government planners implement The Common Approach to Federal Enterprise Architecture. Workstation requirements will help users identify IT standards based on rules or specifications designed to simplify, unify, or rationalize the design, interoperability, portability, and scalability of IT infrastructure components (e.g., network, hardware, systems, and application software).

5. POLICY

All USDA Mission Areas, agencies, and staff offices will comply with the latest version of NIST, [Special Publication \(SP\) 800-53 r5](#), *Security and Privacy Controls for Information Systems and Organizations*; the *E-Government Act*; Circular A-130; Circular A-119; and the FEAF v2 artifacts specifically associated with the Application Reference Model (ARM) and Infrastructure Reference Model (IRM), ensuring that configuration of workstations and peripherals are maintained in accordance with these mandates.

Mission Areas, agencies, and staff offices will comply with this DR by using Departmental, Mission Area, agency, or staff office blanket purchase agreements (BPA) consistent with [Federal Acquisition Regulation \(FAR\) § 13.303](#) that fulfill Common Criteria mandates and are current with voluntary consensus standards. Software and hardware can be authorized for use unless the software developer or hardware developer is prohibited by the law.

- a. When complying with Departmental or agency BPAs, Mission Areas, agencies, and staff offices will:
 - (1) Establish and maintain uniform engineering and technical criteria;
 - (2) Establish and maintain methods, practices, and processes;

- (3) Align with SP 800-53 r5 and *Federal Information Security Modernization Act of 2014 (FISMA)*, [44 U.S.C. § 3551 et seq.](#), security requirements;
 - (4) Establish and maintain net-centric and enhanced interoperable shared services;
 - (5) Develop and establish technical maturity among systems and applications within budgeted limitations;
 - (6) Ensure alignment of investments, systems, and applications to include infrastructure;
 - (7) Manage the replacement of workstations and associated peripherals that are aligned with the current, in-force standards; and
 - (8) Promote best practices in alignment with business, performance, application, infrastructure, data, and security configurations.
- b. Mission Areas, agencies, and staff offices will manage end user (e.g., employees, contractors, USDA partners) computing device allotment and limit the issuance of mobile devices to those with an official business need:
 - (1) End users are limited to one Government-furnished device (workstation or laptop) per individual.
 - (2) End users are allowed only one mobile device, if supported by a business need. An end user cannot have both a mobile phone and a tablet. An exception can be requested for an end user or a group of end users with a demonstrated need, whose position requires both a mobile phone and a tablet.
 - (3) To have a mobile phone or tablet requires the supervisor's approval before either can be issued.
 - c. The point of contact for this policy is the Office of the Chief Information Officer (OCIO), Client Experience Center (CEC) Governance Director, at CEC.InternalComms@usda.gov.

6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO), or delegated responsible staff, will:
 - (1) Be the final approving authority on the adoption of IT requirements and standards for the Department; and
 - (2) Serve as the final approving authority for policy waivers and exceptions to the workstation requirements as requested by Mission Areas, agencies, or staff offices.

- b. The CEC Associate Chief Information Officer (ACIO) will:
 - (1) Develop policies, regulations, and compliance requirements for the IT environment and provide channels for Mission Area, agency, and staff office input to, and approval of, those policies, regulations, and compliance requirements;
 - (2) Monitor and provide recommendations for waivers to this policy to the CIO; and
 - (3) 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 without interfering with or impairing business functions or mission requirements; and
 - (b) Reporting compliance and deviations to OMB.
- c. Mission Area Assistant CIOs and Agency and Staff Office IT Directors will:
 - (1) Implement the policies, requirements, and standards for the IT environment by:
 - (a) Reviewing existing internal procedures and controls and developing internal procedures and controls in support of this policy;
 - (b) Establishing effective communication between internal stakeholders and an identified point of contact in OCIO; and
 - (c) Incorporating the policies, requirements, and standards into Mission Area, agency, 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 the CEC ACIO;
 - (b) Requesting waivers from the CEC ACIO that substantiate all policy exception requirements;
 - (c) Providing corrective action plans for the timely remediation of issues not authorized as an approved deviation;

- (d) Ensuring that all end user peripherals (e.g., storage, network, printers, workstations, mobile devices) necessary for the mission of the user's work pass a comprehensive security scan. Lab workstations are out of scope for this directive. If a peripheral fails a scan and cannot be updated to pass, it is prohibited from being connected to USDA infrastructure, or a waiver must be requested and approved, permitting the scan-failing peripheral to be used in the end user's environment;
 - (e) Procuring hardware and software from enterprisewide BPAs (this does not apply to lab equipment); and
 - (f) Ensuring that Mission Areas, agencies, and staff offices support and participate in the enterprise configuration and change management (ENTCCM) change advisory boards (CAB).
- d. The ENTCCM CAB will:
- (1) Focus on the change and configuration management for USDA enterprisewide end user management. Assist in the maintenance, stability, reliability, and performance of the infrastructure and applications; and
 - (2) Carefully identify, analyze, plan, manage, test, and document ongoing changes at the USDA enterprise and Mission Area, agency, or staff office levels to minimize the possibility of any changes negatively impacting the performance or availability of the enterprise system.

7. POLICY EXCEPTIONS

- a. All USDA Mission Areas, agencies, and staff offices are required to conform to this policy; however, if a specific policy requirement cannot be met as explicitly stated, Mission Areas, agencies, and staff offices may submit a waiver request by an individual or for a functional group, such as Meat Inspector. Submit waiver requests by email to the Category Management Team (SM.OCIO.CIO.Category.Management@usda.gov) with "DR 3170" in the subject line. In the body of the email, present a brief explanation of the violation and explain how a waiver will help business continue.
- b. All appropriate OCIO offices will have the opportunity to comment and provide recommendations prior to the CIO's final decision.
- c. Unless otherwise specified, Mission Areas, agencies, and staff offices will review and renew approved policy waivers every fiscal year. Approved waivers for specialized equipment with a continuing need will be tracked on an approved list. The CEC ACIO will monitor waivers and provide recommendations for waivers to this policy to the CIO.

8. INQUIRIES

Direct all questions concerning this DR by email to the Category Management Team (SM.OCIO.CIO.Category.Management@usda.gov) with “DR 3170” in the subject line.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

ACIO	Associate Chief Information Officer
ARM	Application Reference Model
BPA	Blanket Purchase Agreement
CAB	Change Advisory Board
CEC	Client Experience Center (OCIO component)
CIO	Chief Information Officer
CPIC	Capital Planning and Investment Control
DR	Departmental Regulation
ENTCCM	Enterprise Configuration and Change Management
FAR	Federal Acquisition Regulation
FEAF v2	Federal Enterprise Architecture Framework, Version 2
FISMA	Federal Information Security Modernization Act of 2014
ICS	Industrial Control Systems
IPv6	Internet Protocol Version 6
IRM	Infrastructure Reference Model
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
SP	Special Publication
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

Application Reference Model (ARM). 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 used to operate hardware (e.g., firmware) because these are contained in the IRM. (Source: FEAF v2)

Common Criteria. This governing document provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems. (Source: NIST, SP 800-53 r5)

Infrastructure Reference Model (IRM). The framework and taxonomy-based reference model for categorizing IT infrastructure and the facilities that host and contain the IT infrastructure. (Source: FEAF v2)

Workstation. A desktop computer, a mobile device—such as a laptop computer, mobile phone, or tablet—or another computer or device that accesses the USDA network. (Source: NIST, [SP 800-82 r2](#), *Guide to Industrial Control Systems (ICS) Security*)

APPENDIX C

AUTHORITIES AND REFERENCES

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

The 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, [44 U.S.C § 3601](#), December 17, 2002

Federal Acquisition Regulation (FAR) § 13.303, Blanket purchase agreements (BPAs)

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

NIST, [SP 800-53 r5](#), *Security and Privacy Controls for Information Systems and Organizations*, Revision 5, September 2020, includes updates as of December 10, 2020

NIST, [SP 800-82 r2](#), *Guide to Industrial Control Systems (ICS) Security*, Revision 2, May 2015

OMB, Circular [A-11](#), *Preparation, Submission, and Execution of the Budget*, August 2022

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

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

OMB, [Federal Enterprise Architecture Framework, Version 2](#) (FEAF v2), January 29, 2013

OMB, [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

OMB, [M-17-26](#), *Reducing Burden for Federal Agencies by Rescinding and Modifying OMB Memoranda*, June 15, 2017

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