

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

DEPARTMENTAL REGULATION	Number: DR 3520-002
SUBJECT: Configuration Management	DATE: August 12, 2014
	OPI: Office of the Chief Information Officer – Agriculture Security Operations Center

<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	5
7. Penalties and Disciplinary Actions for Non-Compliance	9
8. Policy Exceptions	9
Appendix A Definitions	A-1
Appendix B Acronyms and Abbreviations	B-1
Appendix C References and Authorities	C-1

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the configuration management policy of the United States Department of Agriculture (USDA or “Department”) for meeting the applicable laws, regulations, and standards of the Federal Government.
- b. This DR addresses guidance issued by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the *Federal Information Security Management Act of 2002 (FISMA)*; requiring federal agencies to include “policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency” within its information security program, and Federal Information Processing Standards Publication ([FIPS PUB](#)) 200, *Minimum Security Requirements for Federal Information and Information Systems*.

- c. It is the policy of USDA to comply with federal requirements to establish, implement, augment, and support configuration management to manage risk to USDA systems.

2. SCOPE

This policy applies to all USDA systems (e.g., mainframes, workstations, servers, databases, electronic mail, authentication, web, proxy, file, domain name systems (DNS), network components, mobile devices, firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors, operating systems, middleware, and applications) developed, maintained, or operated by USDA agencies, staff offices, employees, contractors, and others working for or on behalf of the USDA.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

This policy supersedes the following Departmental directives:

- a. Departmental Manual (DM) 3520-000, *Configuration Management*, dated July 15, 2004;
- b. DM 3520-001, Chapter 4, Part 1, *CM Policy & Responsibilities*, dated July 17, 2004;

4. BACKGROUND

Configuration management is an essential component of monitoring the status of security controls and identifying potential security-related problems in information systems. This information can help security and IT managers understand and monitor the evolving nature of vulnerabilities as they appear in a system under their responsibility, thus enabling managers to direct appropriate changes, as required. Configuration management ensures that the hardware, software, communications services, and documentation for a system can be accurately determined at any time.

Configuration management is conducted throughout the life cycle of the system through an established configuration management process. The configuration management process identifies the steps required to ensure that all changes are properly requested, evaluated, and authorized. The configuration management process also provides a detailed, step-by-step procedure for identifying, recording, evaluating, tracking, coordinating, reporting, and controlling configuration items.

The objectives of configuration management are to:

- a. Provide controls to ensure that the system operates correctly throughout its life;
- b. Ensure that the configuration of all system components is available and accurate at all times;

- c. Ensure that the pertinent functional and physical interfaces among systems, equipment, and software are correctly and adequately documented;
- d. Ensure that the pertinent virtual and logical interfaces among systems, equipment, and software are correctly and adequately documented;
- e. Provide maintenance efficiency by ensuring that change proposals are adequately acted upon; and
- f. Ensure that the impact of any change to system functionality, security, performance, or cost is known at the time the change is approved.

5. POLICY

- a. USDA agencies and staff offices shall integrate configuration management throughout the life cycle of all USDA information systems and DNS.
- b. USDA agencies and staff offices shall ensure that authorized agency personnel evaluate, track, coordinate, report, and approve all changes to system baseline configurations in accordance with [NIST Special Publication \(SP\) 800-100](#), *Information Security Handbook: A Guide for Managers*, guidelines for configuration management and the controls as outlined in FIPS 200 and [NIST SP 800-53](#), Revision 3, *Recommended Security Controls for Federal Information Systems*.
- c. USDA agencies and staff offices shall ensure that configuration control procedures are established to implement this policy.
- d. USDA agencies and staff offices shall apply secure baseline configurations for all hardware and software products used within the USDA network boundary, in alignment with NIST SP 800-53, [NIST SP 800-70](#), Revision 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*; [NIST SP 800-117](#), *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, Version 1.0; [NIST SP 800-126](#), *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*; and [NIST SP 800-128](#), *Guide for Security-Focused Configuration Management of Information Systems*.
- e. USDA agencies and staff offices shall ensure that requirements for deploying Domain Name System Security (DNSSEC) to all federal information systems are in accordance with [OMB M-08-23](#), *Securing the Federal Government's Domain Name System Infrastructure*, [NIST SP 800-81](#), Revision 1, *Secure Domain Name System (DNS) Deployment Guide*, and NIST SP 800-53.
- f. Agencies and staff offices shall use automated configuration monitoring tool(s) to ensure adherence to configuration guidance and during periodic system monitoring.

- g. Agencies and staff offices shall use the most current *United States Government Configuration Baseline* ([USGCB](#)) settings for configuration of laptops, workstations, servers, and the most current NIST National Checklist Program ([NCP](#)) Repository checklists for all other hardware and software.
- h. There are four tiers of NCP checklists, ranging from Tier I (manual) through Tier IV (automated). Agencies and staff offices shall utilize the highest tiered checklist available at the time of system configuration.
- i. If NIST does not have a checklist for the product being used, the vendor's secure baseline configuration or best practice guidance shall be used until NIST issues a checklist in accordance with USDA Agriculture Security Operations Center (ASOC) Oversight and Compliance Division (OCD) Standard Operating Procedure (SOP) [OCD-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*.
- j. Checklists should be tailored by agencies and staff offices to meet their particular security and operational requirements, but shall, at a minimum, meet the security requirements outlined in USGCB settings or NCP checklists.
- k. Configuration settings that are not in compliance with NIST checklists and USGCB settings shall be remediated within 30 days. If they cannot be remediated within the 30 days, agencies and staff offices are required to create a mitigation strategy in the form of a plan of action and milestones (POA&M), as described in [OMB M-04-25](#), *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, and all successive annual FISMA reporting instructions; [OMB M-03-19](#), *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*; [DM 3555-001](#), *Certification and Accreditation Methodology*; the ASOC OCD SOP [OCD-SOP-004](#), *USDA Six Step Risk Management Framework Process Guide (RMF Process Guide)*; and other applicable USDA [Series 3500](#) policies.
- l. All deviations from USGCB settings shall be documented and submitted to the USDA Chief Information Security Officer (CISO) and be approved prior to implementation on agency and staff office production systems.
- m. Agencies and staff offices shall assign qualified staff to be responsible for controlling and approving changes throughout the development and operational life cycle of products and systems.
- n. Agencies and staff offices shall ensure configuration change control processes are developed to ensure that proposed non-emergency changes are evaluated, tested, approved, and documented before being put into production, with potential security impacts considered prior to change implementation.

- o. Agencies and staff offices shall track emergency configuration changes and report them to the configuration control board (CCB), once the emergency change has been implemented.
- p. The original approved baseline configuration and all subsequent changes and revisions shall be made as part of a risk-based decision, tracked, and kept current through documented change control throughout the system life cycle.
- q. Configuration settings shall be tested and approved by appropriately designated personnel as outlined by agency and staff office procedures, before applying them to production systems.
- r. Agencies and staff offices shall establish and maintain a current centralized inventory of approved and unapproved agency and staff office hardware and software.
- s. Agencies and staff offices shall review hardware and software inventory, at a minimum, quarterly.
- t. Agencies and staff offices shall ensure employees, partners, and volunteers are prohibited from downloading software or connecting hardware unless pre-approval has been granted and documented including the duration of use.
- u. Systems connected to the USDA backbone and reported in the USDA's official FISMA data management and reporting tool shall have or be covered by a configuration management plan as outlined in NIST SP 800-128 and the *RMF Process Guide*.
- v. Configuration management requirements shall be included in all applicable statements of work and procurement requests for all contracts involving purchase of USDA systems, hardware, and applications.
- w. All USDA employees, contractors, partners, and volunteers responsible for development or maintenance of USDA systems shall be trained in configuration management in accordance NIST SP 800-128.

6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) shall:
 - (1) Ensure that the Departmentwide information security program incorporates configuration management as part of system life cycle management activities; and
 - (2) Designate a security-focused configuration management (SecCM) program manager for the agencies and staff offices and approve Departmental policies and plans related to configuration management.

b. The USDA CISO shall:

- (1) Report directly to the USDA CIO and serve as the principal advisor for information security matters;
- (2) Implement and manage the USDA Information Technology (IT) Security Program to ensure compliance with applicable federal laws, Executive orders, directives, policies, and regulations;
- (3) Serve as the SecCM program manager or delegate the SecCM program manager responsibilities to another qualified staff member;
- (4) Ensure the development and maintenance of USDA configuration management policies and procedures;
- (5) Provide oversight of USDA agencies and staff offices to ensure implementation of this policy, compliance with NIST configuration checklists, and application of USGCB secure configuration management settings for USDA systems;
- (6) Provide oversight of the agency and staff office security programs to ensure implementation of the NIST configuration checklists and USGCB settings for all USDA systems, as well as meeting OMB requirements for reporting and submission of evidence to support compliance to ensure continuous monitoring of Departmentwide security posture;
- (7) Review and render decision for agency and staff office policy waiver requests; and
- (8) Ensure that this policy is reviewed at least annually for compliance with applicable federal laws, Executive orders, directives, policies, and regulations.

c. Agency and staff office CIOs shall:

- (1) Establish and maintain agency and staff office specific policies, procedures, guidance, processes, and baseline configuration checklists, as appropriate, and assign responsibilities to implement this policy;
- (2) Ensure that staff receives role-based training to carry out their security-related responsibilities as outlined in [DM 3545-001](#), *Computer Security Training and Awareness*;
- (3) Ensure that agencies and staff offices report status to the USDA on configuration management requirements as requested;
- (4) Ensure a current centralized inventory of approved and unapproved agency and staff office hardware and software is maintained;

- (5) Ensure that the centralized inventory is reviewed, at a minimum, quarterly; and
 - (6) Review and submit completed waivers to the USDA CISO for any requirement that is not in compliance with this policy.
- d. Agency and staff office Information Systems Security Program Managers (ISSPMs) shall:
- (1) Oversee agency and staff office system configuration compliance with this policy;
 - (2) Ensure the development of agency and staff office specific policy and procedures necessary to integrate USDA policy into the agency or staff office configuration management activities;
 - (3) Ensure that only agency and staff office approved hardware and software is used within the agency and staff office network boundaries; and
 - (4) Participate in configuration management activities, to include CCBs, as applicable, for agency or staff office owned and operated systems.
- e. Authorizing Officials or the Authorizing Official's Designated Representative shall:
- (1) Manage or participate in the CCBs for relevant systems and provide technical staff, as required, to conduct and/or review security impact analyses; and
 - (2) Coordinate with the Risk Executive (function) on SecCM issues and make the final determination whether or not a given change or set of changes continues to be an acceptable security risk.
- f. Agency and staff office Information System Security Officers shall:
- (1) Ensure system compliance with NIST checklists and USGCB settings; and
 - (2) Assist with compiling applicable agency and staff office reports related to this policy.
- g. Agency and staff office System Owners shall:
- (1) Identify, define, and ensure implementation of NIST checklists and USGCB settings and document secure baseline configurations for all systems under system owner responsibility;
 - (2) Ensure that systems comply with agency and staff office approved hardware and software lists;

- (3) Ensure that change controls are in place and that system/application modifications are conducted in accordance with the change control process as outlined in the configuration management plan and the *RMF Process Guide*; and
 - (4) Ensure that a waiver is submitted to the agency CIO for any requirement that is not in compliance with this policy.
- h. Agency and staff office System Administrators shall:
- (1) Comply with SecCM policies and procedures relevant to the system;
 - (2) Implement secure baseline configurations in accordance with NIST requirements, incorporate secure configuration settings for IT products, assist with security impact analysis, configuration management, and continuous monitoring activities, as needed;
 - (3) Implement and maintain approved baseline configurations for all agency and staff office owned systems;
 - (4) Participate in the configuration management control process to include serving on CCBs, as assigned by agency and staff office leadership; and
 - (5) Identify and report to agency and staff office ISSPMs any non-compliance with approved baseline configurations.
- i. Agency and staff office Software Developers shall:
- (1) Comply with SecCM policies and procedures relevant to each system;
 - (2) Ensure that secure configuration settings are built into applications in accordance with OMB guidance and NIST requirements;
 - (3) Assist with security impact analyses, configuration management, and continuous monitoring activities as needed;
 - (4) Implement and maintain approved baseline configurations for all agency and staff office owned systems; and
 - (5) Participate in the configuration management control process to include serving on CCBs, as assigned by agency or staff office leadership.
- j. Agency and staff office Contracting Officers shall ensure that IT procurements comply with Part 39, Section 39.101, Paragraph (d) of the Federal Acquisition Regulation ([FAR](#)) which states: “In acquiring information technology, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations...”

- k. USDA employees, contractors, and others working for or on behalf of the USDA shall comply with the guidance provided in this policy, as applicable.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

[DM 3300-005](#), *Policies for Planning and Managing Wireless Technologies in USDA*, Chapter 3, sets forth USDA's policies and standards on employee responsibilities and conduct relative to the use of wireless technologies.

[DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16, sets forth the USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment, with further delineation provided in [DR 3300-001](#), *Telecommunications & Internet Services and Use*, Section 3. In addition, DR 4070-735-001, Section 21, Disciplinary or Adverse Action, states:

- a. A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action.
- b. Disciplinary or adverse action shall be effected in accordance with applicable law and regulations.

Such disciplinary or adverse action shall be effected in accordance with applicable law and regulations such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, OMB regulations, and Standards of Conduct for Federal Employees.

8. POLICY EXCEPTIONS

- a. All USDA agencies and staff offices are required to conform to this policy. In the event that a specific policy requirement cannot be met as explicitly stated, the agency or staff office may submit a waiver request. Waiver requests shall explain the reason for the request, identify compensating controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the policy requirement. Agencies and staff offices shall address all policy waiver request memoranda to the USDA CISO and submit the request to asoc.outreach@asoc.usda.gov for review and determination.
- b. Agencies and staff offices shall review and renew approved policy waivers every fiscal year. Approved waivers shall be associated with a NIST security control and tracked as a POA&M item in the Department's FISMA data management and reporting tool. The USDA CISO shall render decision and monitor waivers to this policy.

-END-

APPENDIX A DEFINITIONS

- a. Authentication. Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
(Source: NIST SP 800-53, Revision 3)
- b. Authorizing Official. Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Synonymous with Accreditation Authority.
(Source: NIST Interagency Report (IR) 7298, Revision 2)
- c. Baseline Configuration. A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
(Source: NIST IR 7298, Revision 2)
- d. Configuration Change Control. A process for managing updates to the baseline configurations for the configuration items.
(Source: NIST SP 800-128)
- e. Configuration Control. A process of controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modification prior to, during, and after system implementation.
(Source: NIST IR 7298, Revision 2)
- f. Configuration Control Board (CCB). A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.
(Source: NIST IR 7298, Revision 2)
- g. Configuration Item. An identifiable part of a system (e.g., hardware, software, firmware, documentation, or a combination thereof) that is a discrete target of configuration control processes.
(Source: NIST SP 800-128)
- h. Configuration Management. A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
(Source: NIST SP 800-128)

- i. Configuration Management Plan. A configuration management plan is a comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. The basic parts of a configuration management plan include:
 - (1) CCB;
 - (2) Configuration Item Identification;
 - (3) Configuration Change Control; and
 - (4) Configuration Monitoring.
(Source: NIST SP 800-128)
- j. Configuration Monitoring. A process for assessing or testing the level of compliance with the established baseline configuration and mechanisms for reporting on the configuration status of items placed under configuration management.
(Source: NIST SP 800-128)
- k. Configuration Settings. The set of parameters that can be changed in hardware, software, and/or firmware that affect the security posture and/or functionality of the information system.
(Source: NIST SP 800-128)
- l. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: NIST IR 7298 Revision 2)
- m. Mobile Devices. Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory). Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices.)
(Source: NIST IR 7298 Revision 2)
- n. Risk Executive (Function). An individual or group within an organization that helps to ensure that:
 - (1) Security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and

(2) Managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.

(Source: NIST IR 7298, Revision 2)

o. Security Configuration Checklist. A security configuration checklist (also called a lockdown, hardening guide, or benchmark) is a series of instructions for configuring a product to a particular operational environment. Checklists can comprise templates or automated scripts, patches or patch descriptions, Extensible Markup Language (XML) files, and other procedures.
(Source: NIST SP 800-70)

p. Security-Focused Configuration Management (SecCM). The term security-focused configuration management (SecCM) is used to emphasize the concentration on information security. Though both IT business application functions and security-focused practices are expected to be integrated as a single process, SecCM in this context is defined as the management and control of configurations for information systems to enable security and facilitate the management of information security risk.

(Source: NIST SP 800-128)

APPENDIX B
ACRONYMS AND ABBREVIATIONS

ASOC	Agriculture Security Operations Center
CCB	Configuration Control Board
CI	Configuration Item
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DM	Departmental Manual
DNS	Domain Name System
DNSSEC	Domain Name System Security
DR	Departmental Regulation
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IR	Interagency or Internal Report
ISSPM	Information Systems Security Program Manager
IT	Information Technology
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
OCD	Oversight and Compliance Division
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
PUB	Publication
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol
SecCM	Security-Focused Configuration Management
SOP	Standard Operating Procedure
SP	Special Publication
USDA	United States Department of Agriculture
USGCB	United States Government Configuration Baseline
XML	Extensible Markup Language

APPENDIX C
REFERENCES AND AUTHORITIES

[DM 3300-005](#), *Policies for Planning and Managing Wireless Technologies in USDA*, November 10, 2010

[DM 3545-001](#), Chapter 9, Part 1, *Computer Security Training and Awareness*, February 17, 2005

[DM 3555-001](#), Chapter 11, Part1, *Certification and Accreditation Methodology*, October 18, 2005

[DR 3300-001](#), *Telecommunications & Internet Services and Use*, March 23, 1999

[DR 4070-735-001](#), *Employee Responsibilities and Conduct*, October 04, 2007

Federal Acquisition Regulation ([FAR](#))

[Federal Information Security Management Act of 2002 \(FISMA\)](#), 44 United States Code (U.S.C.) 3541 et seq. (2013)

[FIPS PUB 200](#), *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

[NIST IR 7298](#), Revision 2, *Glossary of Key Information Security Terms*, May 2013

[NIST SP 800-53](#), Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009

[NIST SP 800-70](#), Revision 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, February 2011

[NIST SP 800-81](#), Revision 1, *Secure Domain Name System (DNS) Deployment Guide*, April 2010

[NIST SP 800-100](#), *Information Security Handbook: A Guide for Managers*, October 2006

[NIST SP 800-117](#), *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, Version 1.0, July 2010

[NIST SP 800-126](#), Revision 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, September 2011

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

NIST, [National Checklist Program \(NCP\) Repository](#)

NIST, [The United States Government Configuration Baseline \(USGCB\)](#)

[OCD-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*

[OCD-SOP-004](#), *USDA Six Step Risk Management Framework (RMF) Process Guide*, Revision 2.38, December 2012

[OMB M-02-01](#), *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 17, 2001

[OMB M-03-19](#), *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, August 6, 2003

[OMB M-04-25](#), *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, August 23, 2004

[OMB M-08-23](#), *Securing the Federal Government's Domain Name System Infrastructure*, August 22, 2008

USDA, [Employee Relations Formal Discipline Checklist](#)

USDA Directives [Series 3500](#), *Cyber Security*