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

DEPARTMENTAL REGULATION	NUMBER: DR 3520-002
SUBJECT: Configuration Management	DATE: July 17, 2019
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: July 17, 2024

Section Page

1. PURPOSE

a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy for configuration management, security configuration management (SecCM), which is also known as secure or security-focused configuration management, and inventory management.

b. In addition to configuration management, SecCM, and inventory management, this policy addresses prohibitions or restrictions on functions, services, ports, protocols, and software installation and usage, based on the configuration management (CM) controls in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. These restrictions and prohibitions are necessary to prevent unauthorized connection of devices, unauthorized tunneling, and unauthorized transfer of information that violates copyright laws or affords access to or use of unauthorized or illegal materials.

c. It is the policy of USDA to comply with Federal laws, regulations, and standards to establish, implement, and enforce a configuration management policy to continually manage risks to USDA information resources.

d. This policy complies with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), 44 United States Code (U.S.C.) § 3551; Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*; NIST SP 800-53 Revision 4; NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*; and other Federal laws, regulations, requirements, and standards regarding configuration management.

e. This policy serves as the foundation on which USDA agencies are to develop and implement configuration management plans and procedures for the information systems and services in their area of responsibility.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This policy supersedes the following in their entirety:

(1) DR 3520-002, *Configuration Management*, dated August 12, 2014; and

(2) Department Manual (DM) 3525-002, *Internet Use & Copyright Restrictions*, dated July 15, 2004.

b. This policy is effective immediately and remains in effect until superseded.

c. All USDA agencies will align their policies and procedures with this DR within 6 months of the publication date.

d. This policy complements other Departmental directives that cover similar topics but is written from the information security perspective of the NIST CM control family. This policy addresses monitoring for actual or potential security violations and enforcing compliance to scan for, prevent access to, or use of unauthorized software applications. It also addresses secure configurations and integrating security considerations into configuration management processes. Complementary policies include:

(1) DR 3160-001, *Licensed Information Technology (IT) Software*;

(2) DR 3170-001, *End User Workstation Configurations*;

(3) DR 3180-001, *Information Technology Standards*;

(4) DR 3300-001, *Telecommunications and Internet Services and Use*; and

(5) DM 3300-005, *Policies for Planning and Managing Wireless Technologies in USDA*.

e. This policy closely relates to the following information security directives:

(1) DR 3530-006, *Scanning and Remediation of Configuration and Patch Vulnerabilities*; and

(2) DR 3575-002, *System and Information Integrity*.

f. When this DR states that a setting must comply with a Defense Information System Agency (DISA) Security Technical Implementation Guide (STIG), an equivalent setting from a *United States Government Common Baseline Configuration* (USGCB) setting checklist is also permitted without a waiver. The *National Checklist Program* (NCP) is the U.S. Government repository of publicly available security checklists or benchmarks that provide detailed, low-level guidance for setting the security configuration of operating systems and applications.

g. The term "agencies" or "USDA agencies" will be assumed to generically refer to Mission Areas, agencies, and staff offices unless otherwise specified.

h. The term "USDA employee" means a Federal civil servant employed by, detailed or assigned to, USDA, including members of the Armed Forces.

i. The term "USDA personnel" means USDA employees, contractors, affiliates, interns, fellows, and volunteers who work for, or on behalf of, USDA, and whose work is overseen by USDA employees.

j. The terms "hardware" and "hardware asset" are used in this policy in conformance with Federal guidance for *FY 2018 CIO FISMA Metrics* Version 1.0. A related term is "hardware component." Examples are:

(1) Endpoint devices such as servers, workstations, and laptops;

(2) Mobile devices, such as smartphones and tablets;

(3) Networking devices such as routers, switches, firewalls, wireless access points, intrusion detection/intrusion prevention systems, modems, and network address translators;

(4) Other communication devices such as alarms, physical access control devices, and virtual private networks (VPN);

(5) Network-addressable input and output devices such as printers, copiers, scanners, network accessible storage devices, Voice over Internet Protocol (VoIP) phones, and other network-addressable devices; and

(6) Virtual machines that can be addressed as if they are a separate physical machine.

k. The term “material conflict of interest” means a conflict of interest is considered ‘material’ if a reasonable disinterested person would take it into account in exercising judgment or making a decision.

l. The terms “software,” “software asset,” and “software component” are used in this policy to encompass types of software such as commercial off-the-shelf (COTS) and open-source software including applications, code snippets, and code libraries; operating systems, databases, functional applications, middleware; security-relevant software such as antivirus; custom-developed software; firmware; and software code incorporated by vendors into hardware appliances to perform tasks such as big data analytics or intrusion protection. “Firmware” may be mentioned separately from “software.”

m. The term “vulnerability” is used instead of “flaw” to describe weaknesses in systems or protection mechanisms that must be remediated.

3. BACKGROUND

Configuration management encompasses the planning and processes to manage the impacts of changes or differences on an information system or network and, by extension, on an organization. Configuration management promotes the security objectives of confidentiality, integrity, and availability for information systems and ensures that the state of the hardware, software, communications services, documentation, and other artifacts (all formally referred to as “configuration items”) for a system can be accurately determined at any time. Furthermore, properly managing the inventory of hardware and software assets and the configurations of those assets is an essential factor in monitoring the status of security controls, identifying potential security-related problems in information systems, and reducing the risk of exploitation or inadvertent failures.

Configuration management practices support information security continuous monitoring, which is described in NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*. ISCM provides an up-to-date view of information security risks. For example, outputs of ISCM include security-related information pertaining to the accuracy of the information system component inventory, which in turn is needed for managing remediation of configuration and patch vulnerabilities, reporting metrics to the Office of Management and Budget (OMB), and ongoing authorization of the system.

Understanding the evolving nature of vulnerabilities as they appear in a system can help security managers and system owners to direct appropriate changes. Changes to IT products (hardware and software) include installation or implementation, modification or patching, and deletion or uninstalling. Changes to system-related documentation such as administrator guides, diagrams, and system security plans are also subject to configuration management controls.

Configuration management planning and procedures provide a repeatable mechanism for implementing system modifications in a controlled environment. This allows the established configuration management process to be conducted throughout the lifecycle of the system.

The system lifecycle begins with establishing an initial baseline for all information system components, with subsequent updates to the baseline as controlled changes are implemented.

Configuration change control procedures identify the steps required to ensure that all changes are properly requested, evaluated for both functional and security impacts, and authorized. Configuration management also requires procedures for identifying, recording, evaluating, tracking, coordinating, reporting, and controlling configuration items.

a. General objectives of configuration management are to:

   (1) Provide controls to ensure that the information system operates correctly throughout its life;

   (2) Maintain a current, accurate inventory of the information system and associated documentation as the system changes;

   (3) Ensure that the configurations of all information system components are approved, available to those with a need-to-know, current, complete, and accurate at all times;

   (4) Ensure that the pertinent physical (functional) and logical (virtual) interfaces among systems, equipment, and software are correctly and adequately documented in the System Security Plans (SSP), Interconnection Security Agreements (ISA), and Information System Contingency Plans;

   (5) Promote hardware and software maintenance efficiency by ensuring that change proposals are appropriately acted upon; and

   (6) Ensure that the impact of any change to system functionality, security, privacy, performance, or cost is known at the time the change is approved.

b. SecCM activities include:

   (1) Identification and recording of configurations that impact the security posture of the information system, privacy information, and the organization;

   (2) Consideration of security risks in approving the initial configuration;

   (3) Analysis of security implications of changes to the information system configuration; and

   (4) Documentation of the approved and implemented changes.

c. Inventory scans, also referred to as discovery scans, probe wired or wireless networks, identifying hardware and software assets for inventory purposes, open ports and services running on those ports, and protocols. Vulnerability scans assess compliance with technical security controls, such as identifying configuration issues, missing or out-of-date patches, or other vulnerabilities. Configuration management procedures govern remediation of those vulnerabilities.

d. Some hardware assets, such as network equipment, printers, application appliances, and mainframes, may not support endpoint agents. For these, a different tool must be used to perform agentless scanning. These devices are sometimes termed "non-managed" or "unmanaged" assets, which means an installed agent does not actively manage them, but they still require oversight through other technical or non-technical means. Unmanaged assets must adhere to configuration management procedures.

4. SCOPE

a. This policy applies to:

(1) All USDA agencies and personnel responsible for activities related to configuration management, SecCM, and inventory management;

(2) All information system users with respect to software installation and usage on government furnished equipment (GFE);

(3) All Federal information, in any medium or form, generated, collected, provided, transmitted, stored, maintained, or accessed by, or on behalf of, USDA;

(4) GFE devices such as mobile devices; and

(5) All documentation, diagrams, scripts, custom code, and other artifacts associated with the information system or service.

b. Nothing in this policy will alter the requirements for the protection of information associated with national security systems such as those in FISMA, policies, directives, instructions, and standards issued by the Committee on National Security Systems (CNSS), or the intelligence community.

5. POLICY

a. All information systems and services reported in USDA's official FISMA data management and reporting tool will have or be covered by a configuration management plan that:

(1) Addresses roles and responsibilities;

(2) Describes the configuration change control processes and procedures and their application throughout the information system lifecycle;

(3) Defines the process for identifying and managing the configuration of information system components (which will be included as configuration items in 5a(4));

(4) Defines all configuration items and places them under configuration control; and

(5) Describes establishing and updating secure configuration baselines.

b. Requirements for configuration management, SecCM, and use of mandatory secure configurations will be included in all statements of work and procurement requests for all contracts involving acquisition of:

(1) Hardware and software assets; and

(2) Services for integration, development, maintenance of information systems, software, or hardware components.

c. USDA agencies will establish, implement, and maintain procedures for configuration management, SecCM, inventory management, and change control processes to include:

(1) Robust integration throughout the lifecycle activities of all information systems and services used or operated by, for, or on behalf of USDA;

(2) Tight integration with vulnerability management processes such as software vulnerability remediation, application of security-relevant software updates (e.g., patches, service packs, hot fixes, anti-malware signatures), and system configuration and hardening;

(3) Integration with other processes such as risk assessment and risk management, plans of action and milestones (POA&M), security assessments, continuous monitoring, incident management, and system error handling;

(4) Management of the inventory of hardware and software assets (components or configuration items) and system documentation;

(5) Identifying and reporting high-value assets (HVA), at least annually, to the Information Security Center (ISC) via email to ASOC.Outreach@usda.gov and cyber.incidents@usda.gov;

(6) Identification of secure configurations to be applied;

(7) Monitoring activities (such as through automated scans) to ensure current, complete, and accurate configuration baselines and to detect unauthorized or undocumented changes; and

(8) Developing and reporting metrics for compliance with policy and procedures.

d. Configuration change control procedures and processes will address:

(1) Scheduled changes and upgrades such as modifications to, or removal of, hardware or software components, changes to configuration settings, and opening or closing of ports;

(2) Emergency and time-sensitive changes;

(3) Automated change mechanisms such as patch installations or updates to malicious code protection; and

(4) Unauthorized or undocumented changes that have been discovered, including managing these as vulnerabilities or incidents.

e. Mission Area, agency, and staff office policies (if they exist) and procedures will address processes and any required documentation for:

(1) Proposing and justifying changes;

(2) Reviewing proposed changes and evaluating security, privacy, functional, and other impacts of proposed changes;

(3) Meeting timeframe standards for security-relevant changes based on criteria, such as:

(a) The severity of the vulnerability and compliance with policy and procedures for scanning and remediation of configuration and patch vulnerabilities;

(b) The security categorization of the information system; and

(c) Releases from vendors of malicious code protection mechanisms.

(4) Determining whether a given change or set of changes constitute an acceptable security risk and documentation of the risk-based decision along with requirements for controls to mitigate the risk;

(5) Handling exception requests, such as deviations from required secure configurations and settings, to include the criteria for approving or denying the requests and documenting the decisions;

(6) Determining the degree and type of testing needed for specific types of changes (e.g., no testing of anti-malware signatures; validating vulnerability remediation; or a full security assessment on a mission-critical system), privacy impact for individual privacy, and for the security impact level of the system (e.g., a separate test environment for high-impact systems);

(7) Approving, denying, or deferring proposed changes;

(8) Implementing approved changes and verifying the change was implemented correctly;

(9) Ensuring that supporting and related documentation such as design documents, component inventories, security plans, and POA&Ms are also updated;

(10) Closing change requests; and

(11) Retaining and archiving baselines.

f. The configuration change control processes will be overseen by a duly established configuration control board (CCB) consisting of USDA personnel who:

(1) Are qualified to control and approve proposed changes; and

(2) Do not have a material conflict of interest regarding approving proposed changes.

g. Authority or ability to make changes to information systems, baseline configurations, and the inventory will be limited to qualified, duly authorized USDA personnel through appropriate access control mechanisms.

h. USDA agencies will support the maintenance of the Departmentwide inventory of information systems and information system components by documenting all data elements required by the Department in support of reporting and other activities as follows:

(1) For managed components (those with installed agents), identify, correct, or add components that have incorrect or missing values for the Agency Identification number and Computer Group fields; and

(2) For non-managed components (those without installed agents), maintain a current inventory that includes manually tracked information such as the system name, property number, serial number, contact information for the responsible system owner and system administrator, and physical location information and information collected through an inventory scan.

i. USDA agencies will develop, document, and maintain a current, complete, and accurate inventory and baseline configuration of each information system or service and its components under configuration control and:

(1) Contain no duplicates, ensuring that each component in the inventory falls within the accreditation boundary of only one information system;

(2) Track all assets throughout their lifecycle from acquisition and installation through retirement and removal;

(3) Use established configuration change control processes and reconcile them with the inventory scans to reflect current installations, upgrades, modifications, version or patch levels, remediation of other vulnerabilities, and retirement of components;

(4) Enumerate the hardware and software assets and the configuration settings and parameters for each asset;

(5) Identify the logical placement of components within the system architecture; and

(6) Describe any connectivity-related aspects of the system such as network topology and physical or logical interfaces to other systems.

j. USDA agencies will reconcile the inventory and configuration information reported from inventory, vulnerability, and other scans of their information systems and information system components and, through the configuration change control process, address unresolved issues such as:

(1) The presence of unauthorized hardware or software;

(2) Hardware or software versions that do not conform to the approved baseline;

(3) Configurations or settings that do not conform to Departmental standards or the approved baseline;

(4) Out-of-date or missing patches; and

(5) Out-of-date software, firmware, or software vulnerabilities discovered during security assessments, continuous monitoring, incident response activities, and system error handling.

k. Previous baseline configurations of moderate- and high-impact systems will be retained and archived to support modification rollback or incident investigations.

l. Secure configurations for all hardware and software used within the USDA network boundary will be applied to comply, at a minimum, with Federal and Departmental requirements and guidelines for secure configurations. Agencies may tailor the secure configurations to meet more stringent, but not less stringent security requirements.

m. If not specified in Department policy, hardware and software configuration settings will be applied from a checklist listed on the NIST NCP Repository website, subject to the following requirements:

(1) As the first choice, use the checklist that integrates with an automated tool in a category or, as the last choice, use other checklists that require manual interpretation and integration with an automated tool;

(2) Select a checklist from the Authority dropdown menu in the following preferred order (i.e., if the DISA checklist does not provide the required configuration setting, check the USGCB/TIS, then check other Governmental Authority, and so forth):

(a) Authority = Governmental Authority: Defense Information Systems Agency;

(b) Authority = Governmental Authority: USGCB/TIS;

(c) Authority = any other Governmental Authority selection;

(d) Authority = a Software Vendor selection (e.g., Microsoft, Red Hat); or

(e) Authority = a Third Party selection (e.g., Center for Internet Security, Vanguard Integrity Professionals).

(3) A waiver must be approved by the Associate Chief Information Officer (ACIO) Information Resource Management Center (IRMC), with concurrence by the USDA Chief Information Security Officer (CISO):

(a) For each planned configuration deviation in any checklist listed in Sections 5m(2)(a) or (b); and

(b) To use any checklist listed in Sections 5m(2)(c) through (e).

n. The types of secure configurations applied will be documented not only as part of the configuration control processes and procedures, but also documented in SSPs, system deployment, installation, or administration guides, and contingency plans.

o. Information systems will be configured to provide only essential capabilities and will not permit protocols, ports, services, or functions that present a known risk of exploitation or compromise.

p. Settings identified in Department of Homeland Security (DHS) Binding Operational Directive (BOD) 18-01, *Enhance Email and Web Security* will be included in configuration baseline settings, as appropriate, for publicly accessible Departmental websites and email services.

q. Agencies will perform information system configuration reviews at least monthly, after an incident, and as part of installations and upgrades to identify weaknesses such as information systems not being hardened or configured according to security policies.

r. Agencies will monitor for, prevent, or otherwise enforce USDA policies on the download, installation, or use of unauthorized software applications and files, such as peer-to-peer (P2P), or free or open source encryption software.

s. Agencies will apply blacklisting techniques on moderate-impact systems to identify unauthorized software and prevent execution of such unauthorized software.

t. Application whitelisting techniques will be applied to high-impact systems.

u. Agencies will ensure that use of software and associated documentation complies with copyright laws, contract agreements, software licensing agreements, and digital rights management controls, consistent with DR 3160-001.

v. Agencies will ensure that USDA personnel are prohibited from downloading software or connecting hardware to USDA information systems or networks unless pre-approval has been granted and documented, including the duration of use of the software or hardware. The procedures for requesting software downloads and hardware connections will be documented and appropriately distributed.

w. Prohibitions and restrictions on unauthorized applications and files will be enforced through means such as:

(1) Having all information system users formally acknowledge rules of behavior, at least annually, as part of information security awareness training;

(2) Displaying official USDA warning banners (system use notifications) before granting access to a information system; and

(3) Scanning to monitor user or device accesses and activities and logging actual or potential unauthorized accesses and activities.

6. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) will:

(1) Designate a Departmental SecCM program manager, whose duties may be filled by the USDA CISO or a senior manager who reports to the USDA CISO;

(2) Approve the Departmental SecCM plan and policy; and

(3) Provide ongoing funding for the Departmental program and associated resources for configuration management, SecCM, and inventory management.

b. The USDA CISO will:

(1) Ensure the development, implementation, and maintenance of the Departmental program for configuration management, SecCM, and inventory management and associated procedures to implement this policy and the program;

(2) Serve as the Departmental SecCM program manager, if designated by the USDA CIO;

(3) Develop and disseminate configuration management, SecCM, and inventory management policy and guidance to Mission Area Assistant CIOs, Mission Area Assistant CISOs, and Information Systems Security Program Managers (ISSPM);

(4) Oversee the Departmentwide standards, processes, and techniques for blacklisting and whitelisting;

(5) Ensure all USDA agencies implement and comply with Federal and Departmental requirements for configuration management, SecCM, and inventory management, including:

(a) Integration with information system lifecycle management, risk assessment and risk management, scanning and remediation of configuration and patch vulnerabilities, POA&Ms and waiver requests, and security assessments;

(b) Collecting and maintaining current, complete, and accurate inventory information about Departmental information systems and components;

(c) Implementing secure configurations from the DISA STIGs or, if necessary, other checklists in the NCP Repository; and

(d) Continuous monitoring of configurations and settings with automated scanning tools, reporting results to the ISC Security Integration Division, and timely remediation of findings;

(6) Ensure that required metrics and other information relevant to configuration management, SecCM, and inventory management are regularly collected, analyzed, reported, and then used to improve all aspects of the Departmental program;

(7) Ensure that USDA's inventory of HVAs and their public-facing internet protocol (IP) address ranges are provided to the DHS;

(8) Ensure continuous scanning and monitoring of all USDA networks and information systems to detect unauthorized connections, tunneling, and unauthorized activities, including downloads of unauthorized applications and files from websites for installation on USDA information systems;

(9) Support Mission Areas, agencies, staff offices, the Office of the Inspector General (OIG), and law enforcement in the resolution of all instances of unauthorized use of the internet, copyright infringement, or illegal activities;

(10) Ensure that software use and associated documentation is consistent with contract agreements and copyright laws, including tracking license usage quantities; and

(11) Ensure development and maintenance of the USDA inventory of HVAs and their public-facing IP address ranges and automated methods and procedures for reporting this information to DHS.

c. The ACIO IRMC will coordinate with the USDA CISO or selected designee to review and ensure compliance with the DISA STIG requirements and adjudicate requests for waivers from those requirements.

d. The USDA SecCM Program Manager will:

(1) Develop and maintain the Departmental SecCM plan and procedures;

(2) Oversee implementation of the SecCM program across the Department;

(3) Provide direction and guidance on SecCM to all USDA agencies, as needed; and

(4) Ensure that DHS is provided with USDA's inventory of HVAs and their public-facing IP address ranges.

e. The OIG Office of Investigations will respond to reported incidents of downloading, installing, using, distributing, or reproducing unapproved, unauthorized, illegal, or illegally obtained applications or files or copyright infringement.

f. Mission Area Assistant CIOs will:

(1) Fund and ensure development, implementation, and maintenance of resources and capabilities for configuration management, SecCM, and inventory management;

(2) Provide oversight of Mission Area, agency, and staff office compliance with Federal and Departmental regulations, requirements, standards, and guidance on configuration management, SecCM, and inventory management;

(3) Ensure that USDA personnel with configuration management, SecCM, and inventory management responsibilities within the Mission Area scope of authority are qualified, duly authorized, and held accountable for performing their responsibilities;

(4) Ensure that organizations within the Mission Area develop, document, implement, review, and update procedures for configuration management, SecCM, and inventory management consistent with Federal and Departmental requirements;

(5) Ensure coordination between organizational and Departmental processes and activities for inventory management, configuration management, SecCM, and scanning and remediation of configuration and patch vulnerabilities;

(6) Ensure a current, complete, and accurate centralized inventory of managed and unmanaged hardware and software is maintained, reviewed at least quarterly, and reconciled regularly with Departmental inventory records; and

(7) Ensure that secure configurations and settings are:

(a) Applied to comply with Federal and Departmental standards;

(b) Maintained for information systems and information system components;

(c) Monitored using automated scanning tools; and

(d) That any findings from scans are remediated in a timely manner.

g. Mission Area Assistant CISOs will:

(1) Disseminate Departmental policy, plans, and procedures for configuration management, SecCM, and inventory management, ensuring that these activities are effectively implemented and integrated with each other and with other activities such as information system lifecycle management and vulnerability management;

(2) Oversee compliance with Federal and Departmental requirements for configuration management, SecCM, and inventory management, including:

(a) Security and privacy impact analyses;

(b) Proper maintenance of information system and information system component inventory information;

(c) Implementation and maintenance of secure configurations and settings from DISA STIGs for hardware and software;

(d) Regular information system configuration reviews and prompt remediation of identified weaknesses; and

(e) Use of only approved hardware and software within the information system and network boundaries.

(3) Ensure that procedures for configuration management, SecCM, and inventory management are developed, documented, implemented, and maintained.

h. ISSPMs will:

(1) Ensure the implementation of standards, processes, and techniques for approved software lists and for blacklisting and whitelisting software applications;

(2) Ensure that procedures for requesting software downloads and hardware connections or changes are documented, distributed to all USDA agency stakeholders, and are implemented, enforced, and updated as needed;

(3) Ensure that access restrictions for changes to information systems are limited to qualified, duly authorized USDA personnel and properly enforced; and

(4) Participate in activities for configuration management, SecCM, and inventory management, to include CCBs to determine if requested changes significantly affect authorization and require re-assessment and re-authorization;

(5) Document and distribute procedures for requesting software downloads and hardware connections;

(6) Ensure that POA&Ms and waiver requests are properly documented, submitted, and managed when there is nonconformance with requirements for configuration management, SecCM, or inventory management;

(7) Define approved hardware and software lists, that conforms to Departmental regulations and standards, for use within the agency or staff office;

(8) Ensure that software and associated documentation is used in accordance with contract agreements and copyright laws, including tracking license usage quantities;

(9) Ensure that ISAs, Memorandums of Understanding (MOU), or Memorandums of Agreement (MOA) for interconnected systems are kept current, accurate, and include requirements for configuration management, SecCM, and inventory management; and

(10) Ensure that personnel within their area of responsibility and have responsibilities for configuration management, SecCM, and inventory management are aware of and understand Federal and Departmental requirements.

i. Authorizing Officials will:

(1) Manage or participate in the CCBs for the systems they authorize;

(2) Provide technical staff as needed to conduct or review security impact analyses;

(3) Coordinate with the Department's SecCM program manager on SecCM issues; and

(4) Make the final determination on whether the following conditions constitute, or continue to be (referring to previously implemented changes or accepted deviations), acceptable security risks:

(a) A given change or set of changes;

(b) Deviations from secure configurations and settings such as the DISA STIGs; and

(c) Downloading software or connecting hardware as exceptions to the approved software and hardware lists.

j. System Owners will:

(1) Ensure statements of work and procurement requests for all acquisition contracts for IT products and services for integration, development, or maintenance of information systems, software, and hardware components include requirements for configuration management, SecCM, and use of mandatory secure configurations;

(2) Ensure adequate budgeting for configuration management, SecCM, and inventory management activities for each system;

(3) Designate configuration managers to systems for which they are responsible;

(4) Ensure that each FISMA reportable system has or is covered by a current configuration management plan;

(5) Document the configuration management, SecCM, and inventory management activities and the software that is to be blacklisted or whitelisted in each information system's security plan;

(6) Identify and ensure verified implementation of secure configurations and settings from the DISA STIGs;

(7) Ensure that any planned deviation from secure configurations and settings from the DISA STIGs have approval from the ACIO IRMC and concurrence of the USDA CISO, or selected designee, before implementation;

(8) Ensure that system implementations comply with the approved hardware and software lists;

(9) Ensure that inventory scan information is properly reconciled and documentation is updated to reflect the current status; and

(10) Ensure that POA&Ms are entered in the Department's FISMA data management and reporting tool and, if necessary, that waivers are requested for nonconformance with configuration management, SecCM, or inventory management requirements.

k. Information Systems Security Officers and Information Stewards will:

(1) Assist the system owner with configuration management, SecCM, and inventory management activities, such as:

(a) Identifying secure configurations and settings from the DISA STIGs; and

(b) Documenting justification for deviations from the DISA STIGs and the proposed mitigating controls for submission to the USDA CISO.

(2) Monitor and report on configuration management, SecCM, and inventory management activities, including security configuration reviews; and

(3) Serve on system CCBs, if requested.

l. Configuration Managers will:

(1) Manage the configuration management, SecCM, and inventory management activities for each system;

(2) Develop, implement, and maintain configuration management plans for each FISMA reportable system;

(3) Identify and document each system's hardware, software, interfaces and interconnections, and system documentation as configuration items;

(4) Formally document, implement, and maintain CCB procedures that conform with this policy;

(5) Convene and facilitate CCB meetings and document all decisions of the CCB, including deviations from secure configurations and settings;

(6) Ensure that configuration change control processes are followed when applying patches and remediating other vulnerabilities;

(7) Limit access to baseline configurations and inventory information by other USDA personnel based on job responsibilities and need-to-know;

(8) Establish, document, and maintain current, complete, and accurate configuration baselines and inventories of information system components;

(9) Maintain the centralized inventory of information systems and information system components under their purview, ensuring that all data elements are current, complete, and accurate with respect to the Departmentwide inventory; and

(10) Retain and archive previous baseline configurations of moderate- and high-impact level systems.

m. CCBs will:

(1) Follow procedures established by the configuration manager and comply with Federal and Departmental requirements for configuration management, SecCM, and inventory management; and

(2) Review and address issues such as unauthorized hardware or software, deviations from security requirements of the USGCB settings and NCP Repository checklists, and software vulnerabilities, through the configuration change control process.

n. Network, System, Database, and Application Administrators will:

(1) Comply with, implement, and follow policy and procedures for configuration management, SecCM, and inventory management;

(2) Implement agreed-upon secure baseline configurations and incorporate secure configuration settings for hardware and software;

(3) Install patches and other vulnerability fixes (such as correcting misconfigurations) in compliance with configuration change control processes;

(4) Contribute to documenting configurations and configuration settings;

(5) Assist in determining the appropriate baseline configuration for relevant information system components;

(6) Participate in testing changes before and after implementation;

(7) Participate in configuration change control processes to include assisting with security impact analyses, serving on CCBs, and configuration monitoring activities, when assigned such duties;

(8) Apply and maintain the appropriate application blacklisting or whitelisting techniques when configuring information systems; and

(9) Identify and report issues to CISOs and ISSPMs (e.g., non-compliance with approved baseline configurations, the presence of unauthorized hardware or

connections, suspected violations of copyright protections, or the presence, downloading, or installation of unauthorized software).

o. System and Software Developers and Integrators will:

(1) Comply with, implement, and follow USDA policy and procedures for configuration management, SecCM, and inventory management;

(2) Ensure that secure configurations and settings are built into information systems and applications in accordance with Federal and Departmental requirements;

(3) Implement and maintain approved baseline configurations for all information systems and applications;

(4) Contribute to documenting configurations and configuration settings;

(5) Assist in determining the appropriate baseline configuration for relevant information system components (also referred to as configuration items);

(6) Participate in testing changes before and after implementation; and

(7) Participate in configuration change control processes, to include assisting with security impact analyses, serving on CCBs, and configuration monitoring activities, when assigned such duties.

p. Contracting Officers will:

(1) Consult with the requiring official to ensure the appropriate standards for secure configurations are incorporated in acquisitions of IT products; and

(2) Consult with the requiring official to ensure that appropriate information security policies and requirements for configuration management, SecCM, and inventory management are incorporated in acquisitions of services for integration, development, or maintenance of information systems, software, and hardware components.

q. Information Systems and Services Users will:

(1) Not download, install, use, distribute, or reproduce unapproved, unauthorized, illegal, or illegally obtained applications, files, or copyrighted material (e.g., software, publications, music, photographs, videos, movies) on USDA information systems or devices;

(2) Comply with Federal and Departmental requirements to submit written requests justifying the need or use of non-standard software or hardware (including the duration of use), to obtain approval prior to installing the software or connecting the hardware to USDA information systems or networks; and

(3) Comply with requirements for configuration management, SecCM, and inventory management when requesting changes to information systems.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DR 4070-735-001, *Employee Responsibilities and Conduct*, Section 16, sets forth USDA policy, procedures, and standards on employee responsibilities and conduct regarding the use of computers and telecommunications equipment. 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; and

b. Disciplinary or adverse action will be affected in accordance with applicable law and regulations.

Such disciplinary or adverse action will be consistent with applicable law and regulations, such as Office of Personnel Management regulations, OMB regulations, and the *Standards of Ethical Conduct for Federal Employees of the Executive Branch*.

8. POLICY EXCEPTIONS

a. All USDA agencies are required to conform to this policy. If a policy requirement cannot be met as explicitly stated, a waiver may be requested. Note that an approved waiver does not bring the information system into compliance with policy. Requests for waivers:

(1) Are an acknowledgement of an information system's non-compliance with policy and that an acceptable plan to remediate the weakness has been provided and will be implemented; and

(2) Must be documented as indicated in CAPE-SOP-003, *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1.

b. Policy waiver request memoranda will be addressed to the USDA CISO and submitted to ISC.Outreach@wdc.usda.gov for review and decision. Unless otherwise specified, approved policy waivers must be reviewed and renewed every fiscal year.

9. INQUIRIES

Address inquiries concerning this DR to the Office of the Chief Information Officer, ISC via email to the cscc@ocio.usda.gov mailbox.

-END-

APPENDIX A

AUTHORITIES AND REFERENCES

CNSS, Instruction 4009, *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015

DHS, *Federal Information Security Modernization Act*, web page with current and recent FISMA metrics required by OMB and DHS

DHS, *FY 2018 CIO FISMA Metrics, Version 1.0*, October 31, 2017

DHS, Binding Operational Directive BOD-18-01, *Enhance Email and Web Security*, October 16, 2017

Federal Acquisition Regulation, Title 48 of the Code of Federal Regulations (CFR) Part 39.101, *Policy* (1984, as amended)

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

NIST, FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

NIST, Computer Security Resource Center, *Glossary*

NIST, National Vulnerability Database, *National Checklist Program Repository*

NIST, SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, August 2002

NIST, SP 800-52 Revision 1, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, April 2014

NIST, SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 with updates as of January 22, 2015

NIST, SP 800-70 Revision 4, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers*, February 2018

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

NIST, SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011

NIST, SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011

NIST, SP 800-167, *Guide to Application Whitelisting*, October 2015

NIST, *The United States Government Configuration Baseline*, updated March 28, 2018

Office of Government Ethics, *Standards of Ethical Conduct for Federal Employees of the Executive Branch*, 5 CFR 2635, et seq., (2018)

OMB, Memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*, June 1, 2007

OMB, M-15-13, *Policy to Require Secure Connections across Federal Websites and Web Services*, June 8, 2015

OMB, M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 30, 2015

OMB, M-16-12, *Category Management Policy 16-1: Improving the Acquisition and Management of Common Information Technology: Software Licensing*, June 2, 2016

OMB, M-17-09, *Management of Federal High Value Assets*, December 9, 2016

USDA, CAPE-SOP-003, *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1, November 2015

USDA, CAPE-SOP-004, *USDA Six-Step Risk Management Framework (RMF) Process Guide*, Revision 3.0, December 2016

USDA, DM 3300-005, *Policies for Planning and Managing Wireless Technologies in USDA*, November 10, 2010

USDA, DR 3160-001, *Licensed Information Technology (IT) Software*, May 16, 2019

USDA, DR 3170-001, *End User Workstation Configurations*, May 12, 2015

USDA, DR 3180-001, *Information Technology Standards*, May 12, 2015

USDA, DR 3300-001, *Telecommunications & Internet Services and Use*, March 18, 2016

USDA, DR 3530-006, *Scanning and Remediation of Configuration and Patch Vulnerabilities*, June 5, 2019

USDA, DR 3575-002, *System and Information Integrity*, August 17, 2018

USDA, DR 4070-735-001, *Employee Responsibilities and Conduct*, October 4, 2007

APPENDIX B

DEFINITIONS

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, SP 800-128)

Blacklisting. The process used to identify: (a) software programs that are not authorized to execute on an information system; or (b) prohibited Universal Resource Locators (URL)/websites. (Source: NIST, SP 800-53 Revision 4)

Common Secure Configuration. A recognized standardized and established benchmark (e.g., National Checklist Program) that stipulates specific secure configuration settings for a given IT platform. (Source: NIST, SP 800-128)

Configuration. The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged. (Source: NIST, SP 800-128)

Configuration Control. Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation. (Source: NIST, SP 800-128)

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 lifecycle of an information system. (Source: NIST, SP 800-128)

Configuration Item. An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process. (Source: NIST, SP 800-128)

Configuration Management (CM). 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 lifecycle. (Source: NIST, SP 800-128)

Configuration Management Plan. A comprehensive description of the roles, responsibilities, policies, and procedures that apply when managing the configuration of products and systems. (Source: NIST, SP 800-128)

Configuration Monitoring. 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)

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)

High Value Asset (HVA). Those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically-motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government. (Source: OMB, M-16-04)

Information System Component. A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial IT products. (Source: NIST, SP 800-53 Revision 4)

Information System Component Inventory. A descriptive record of components within an information system. (Source: NIST, SP 800-128)

National Checklist Program Repository. A publicly available resource that contains information on a variety of security configuration checklists for specific IT products or categories of IT products. (Source: NIST, SP 800-70 Revision 4)

Need-to-know. A determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. (Source: NIST, Computer Security Resource Center (CSRC), *Glossary*)

Remediation. The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application. (Source: NIST, CSRC, *Glossary*)

Security Configuration Management (SecCM). The management and control of configurations for an information system to enable security and facilitate the management of risk. (Source: NIST, SP 800-128)

Security Impact Analysis. The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system. (Source: NIST, SP 800-53 Revision 4)

Security Technical Implementation Guide (STIG). Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product which have been selected on a DoD baseline. (Source: CNSS, Instruction 4009)

United States Government Configuration Baseline (USGCB). The USGCB provides security configuration baselines for IT products widely deployed across Federal Agencies. The USGCB baseline evolved from the *Federal Desktop Core Configuration* mandate. The

USGCB is a Federal Governmentwide initiative that provides guidance to Agencies on what should be done to improve and maintain effective configuration settings focusing primarily on security. (Source: NIST, SP 800-128)

Whitelisting. The process used to identify: (a software program that are authorized to execute on an information system; or (b) authorized Universal Resource Locators (URL)/websites. (Source: NIST, SP 800-53 Revision 4)

APPENDIX C

ACRONYMS AND ABBREVIATIONS

ACIO	Associate Chief Information Officer
BOD	Binding Operational Directive
CCB	Configuration Control Board
CFR	Code of Federal Regulations
CM	Configuration Management
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
COTS	Commercial Off-the-Shelf
CSIP	Cybersecurity Strategy and Implementation Plan
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DM	Departmental Manual
DoD	Department of Defense
DR	Departmental Regulation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
GFE	Government Furnished Equipment
HVA	High-Value Asset
IP	Internet Protocol
IRMC	Information Resource Management Center
ISA	Interconnection Security Agreement
ISC	Information Security Center
ISCM	Information Security Continuous Monitoring
ISSPM	Information Systems Security Program Manager
IT	Information Technology
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
P2P	Peer-to-Peer
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol
SecCM	Security Configuration Management
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TIS	Technology Infrastructure Subcommittee, as in USGCB/TIS

TLS	Transport Layer Security
URL	Universal Resource Locator
U.S.C.	United States Code
USDA	United States Department of Agriculture
USGCB	United States Government Configuration Baseline
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network