

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

DEPARTMENTAL REGULATION	NUMBER: DR 3530-006
SUBJECT: Scanning and Remediation of Configuration and Patch Vulnerabilities	DATE: June 5, 2019
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: June 5, 2024

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	2
3. Background	3
4. Scope	4
5. Policy	5
6. Roles and Responsibilities	9
7. Penalties and Disciplinary Actions for Non-Compliance	14
8. Policy Exceptions	15
9. Inquiries	15
Appendix A Authorities and References	A-1
Appendix B Definitions	B-1
Appendix C Acronyms and Abbreviations	C-1

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy to scan for, identify, and remediate inventory, configuration, and patch vulnerabilities.
- b. It is USDA policy to comply with Federal requirements to establish, implement, and support activities pertaining to vulnerability scanning and remediation to continually manage risks impacting USDA information resources.
- c. This policy complies with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), [44 United States Code \(U.S.C.\) § 3551](#); Office of Management and Budget (OMB) Circular [A-130](#), *Managing Information as a Strategic Resource*; National Institute of Standards and Technology (NIST) [Special Publication \(SP\) 800-53 Revision 4](#), *Security and Privacy Controls for Federal Information Systems and Organizations*; and NIST [SP 800-40 Revision 3](#), *Guide to Enterprise Patch Management Technologies*.

- d. This policy serves as the foundation to which Mission Areas, agencies, and staff offices will develop and implement their own policies and procedures for vulnerability scanning and remediation.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy supersedes the following directives in their entirety:
 - (1) Departmental Manual (DM) 3530-001, Chapter 6, Part 1, *Vulnerability Scan Procedures*, dated July 20, 2005;
 - (2) DM 3530-001-01, Amendment Number 1 to Departmental Manual, Chapter 6, Part 1, *Vulnerability Scan Procedures*, dated July 20, 2005; and
 - (3) DM 3535-002, Chapter 7, Part 2, *Patch Management and Systems Updates*, dated May 11, 2005.
- b. This policy is effective immediately when published and will remain in effect until superseded or expired.
- c. All Mission Areas, agencies, and staff offices will align their procedures with this DR within 6 months of the publication date.
- d. The term “finding” applies to any outcome or result discovered that presents a potential information security risk.
- e. The term “artifacts” describes scanning tool outputs, discrepancies between Department, agency, and staff office scans, remediation activities, and POA&Ms that support the execution of scans and remediation activities. Executive summaries of scanning tool reports qualify as artifacts, as proof of scanning activities. However, the full scan report details should be retained as they may be required as supporting artifacts for audits, incident investigations, or Department oversight activities.
- f. The terms “hardware” and “hardware asset” are used in this document to conform to [FY 2018 CIO FISMA Metrics](#) guidance. The categories of hardware assets and examples are:
 - (1) Endpoint devices (e.g., servers, workstations, and virtual machines);
 - (2) Mobile devices (e.g., smartphones, tablets, and pagers);
 - (3) Networking devices (i.e., routers, switches, firewalls, wireless access points, intrusion detection/intrusion prevention systems, modems, and network address translators, etc.); and
 - (4) Other input/output communication devices (i.e., industrial control systems, printers and multifunctional devices, network accessible storage devices, etc.);

- g. The term “Information Security Center (ISC) Alert” (formerly the Agriculture Security Operations Center (ASOC) Alert) refers to an electronic message, sent by ISC describing a critical vulnerability or weakness and recommending mitigation. ISC Alerts may also provide threat information for situational awareness, or that may adversely affect USDA information systems.
- h. The term “mitigation” means the application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences.
- i. The terms “software” and “software asset” are used in this document to encompass types of software including commercial off-the-shelf (COTS) software; open-source software including applications, code snippets, and code libraries; operating systems, databases, functional applications, and middleware; security-relevant software such as anti-virus; custom-developed software; firmware; and software code incorporated into hardware appliances to perform tasks such as big data analytics or intrusion protection. “Firmware” may be mentioned separately from “software.”
- j. The term “USDA employee” refers to a Federal civil servant employed by, detailed or assigned to, USDA, including members of the Armed Forces.
- k. The term “USDA personnel” encompasses employees, contractors, partners, interns, fellows, affiliates, and volunteers.
- l. The term “weakness” is a shortcoming or imperfection in software code, design, architecture, or deployment that, under proper conditions, could become a vulnerability or contribute to the introduction of vulnerabilities.
- m. The terms “zero-day exploit” or “zero-day vulnerability” refer to a flaw or weakness in software that is unknown to the vendor at the time of discovery. Zero-day exploits usually require monitoring or mitigating activities until a remedy is made available.

3. BACKGROUND

Scanning for and managing inventory, patch, and configuration issues are security practices designed to proactively identify and remediate technical vulnerabilities and weaknesses in information systems. Proactively managing and remediating vulnerabilities reduces or eliminates the potential for exploitation and involves considerably less time and effort than responding after exploitation has occurred. In addition, timely patching and fixing configuration issues are essential to maintaining the availability, confidentiality, and integrity of USDA information resources.

These security practices must be ongoing and cyclical to keep pace with the deployment of new or modified information systems and the discovery of new vulnerabilities and weaknesses. The practices are required for production systems and for the deployment of new, upgraded, or modified systems. For production systems, scanning for vulnerabilities and remediating identified vulnerabilities are required activities at least monthly. For new, upgraded, or modified systems, the activities must occur before deployment to production.

This document focuses on scanning to detect and identify:

- a. Wired or wireless devices on USDA network segments, determining which devices are authorized, and those which may be unauthorized or rogue devices;
- b. Attributes of the devices, such as their configuration, open ports and protocols, network services, applications that run those services, operating systems, and major commercial applications; and
- c. Misconfigurations, unauthorized services and protocols, insecure ports, and missing or out-of-date patches.

Some inventory and vulnerability scanning tools interact with agents installed on hardware endpoints. That interaction permits agent-based scanning and management of the devices, their operating systems, and certain software applications. Devices with installed agents are considered managed assets. Managed assets have their vulnerabilities, patches, and configurations detected via an installed agent.

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.

To classify the vulnerabilities found through scanning, USDA uses the vulnerability scanning levels of low, moderate, high, and critical. The severity levels determine the priorities for remediating the vulnerabilities. Common remediation methods include installing security patches for operating systems and major commercial applications, hardening actions (e.g., implementing more stringent configuration settings, fixing misconfigurations, disabling unnecessary or unauthorized services), and closing insecure or unauthorized opened ports.

Remediation activities and timelines should be the result of collaborative stakeholder efforts. POA&Ms document that effort and are used to prioritize and monitor the progress of corrective activities when remediation activities take longer than 30 days.

4. SCOPE

- a. This policy applies to all:
 - (1) Mission Area, agency, and staff office personnel, and others working for, or on behalf of, USDA who are responsible for or involved in conducting information system scans, vulnerability scanning and remediation activities, managing vulnerabilities, ensuring systems are patched, or any of the procedures, plans, and functions thereof;
 - (2) All Federal information, in any medium or form, generated, collected, provided, transmitted, stored, maintained, or accessed by, or on behalf of, USDA;

- (3) Information systems or services (including cloud-based services) used or operated by USDA, USDA contractors, or other organizations on behalf of, or funded by, USDA and interconnections between or among systems or services; and
 - (4) Facilities from which these information systems or services operate, whether owned or operated by USDA, or owned or operated on behalf of USDA by a contractor, subcontractor, or other organization.
- b. This document is closely related to other information security policies, programs, and procedures, including risk assessment and management, configuration management, security assessments, plans of action and milestones (POA&M), and the waiver request process documented in the Departmental standard operating procedure (SOP) by the Compliance and Policy Branch, [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*.
 - c. The following are outside the scope of this document:
 - (1) Requirements for information system monitoring (such as with intrusion detection systems), including information security continuous monitoring;
 - (2) Requirements for auditing and audit log management;
 - (3) Incident management, protection against malicious code, and scanning of removable media; and
 - (4) Certain techniques and activities for identifying threats and vulnerabilities (e.g., application security testing and assessment, malicious code scanning, scanning for indicators of compromise, spam detection, file integrity checking, intrusion detection, identifying rogue connections to or from external information systems).
 - d. Nothing in this policy alters the requirements for the protection of information associated with national security systems such as those identified in FISMA, policies, directives, instructions, and standards issued by the Committee on National Security Systems (CNSS), or the Intelligence Community.

5. POLICY

- a. Only inventory and vulnerability scanning tools that are compliant with the NIST Security Content Automation Protocol (SCAP) specification suite will be used on any USDA network to support official reporting requirements. Other tools approved for use by the Authorizing Official (AO) may be used at Mission Area, agency, or staff office discretion for comparison to official scan reports.
- b. All hardware assets capable of supporting an installed agent will be so equipped, to support Departmental scanning, patching, and inventory management requirements.

- c. Mission Areas, agencies, and staff offices will either perform their own inventory, configuration, and vulnerability scans, contract with a third party (e.g., contractor), or obtain scanning services from ISC or the Agriculture Security Operations Division (ASOD).
- d. USDA personnel will only perform scans on non-USDA Internet Protocol (IP) addresses (e.g., cloud solutions, third-party systems), or USDA IP addresses of other USDA Mission Areas, agencies, or staff offices across network boundaries when permitted to do so by a Memorandum of Understanding (MOU) or contract authorizing such scans.
- e. Only authorized personnel with appropriate background investigations, training, and qualifications will perform scans.
- f. Monthly recurring scan schedules, if applicable, will be provided to ASOD and will include IP ranges, beginning and end dates for each scheduled scan each month. Non-scheduled scans, when feasible, will be coordinated with ASOD via email (cyber.incidents@usda.gov) at least 24 hours prior to conducting any scan activities.
- g. Mission Areas, agencies, and staff offices that perform their own inventory scans will collaborate with ISC to resolve incorrect or missing values and discrepancies between the official USDA inventory of components and the results of their monthly inventory scans by:
 - (1) Obtaining and validating Department-provided inventory data from ISC;
 - (2) Ensuring that Department, Mission Areas, agency, or staff office monthly inventory scans collectively include all hardware and software assets; and
 - (3) Providing required monthly Mission Area, agency, or staff office inventory scan data and any corrections to the Department-provided inventory data to ISC via email to ISC.Outreach@wdc.usda.gov.

Inventory scans conducted by Mission Areas, agencies, and staff offices do not need to include assets included in Department scans. The goal is to achieve comprehensive inventory awareness between the Department, Mission Areas, agencies, and staff offices.

- h. When inventory scans detect unauthorized hardware or software components, Mission Areas, agencies, and staff offices will promptly:
 - (1) Isolate the unauthorized components by disconnecting them from all network access; and
 - (2) Notify the ASOD Cybersecurity Incident Response Team (CSIRT) via email at cyber.incidents@asoc.usda.gov.

- i. When inventory scans detect authorized but undocumented hardware or software components, Mission Areas, agencies, and staff offices will follow their configuration management procedures and processes to incorporate components into the baseline.
- j. Vulnerability scans will:
 - (1) Include all available hardware and software assets; and
 - (2) Enumerate all open ports, protocols, and services listening on systems, to ensure compliance with [DM 3530-004](#), *Firewall Technical Security Standards*; [DR 3520-002](#), *Configuration Management*; and the Mission Area, agency, or staff office system baseline.
- k. Vulnerability scans will be run as fully credentialed, when supported, using an account to authenticate to each scanned system or application and with the scanning tool up-to-date (within 7 calendar days) with the following:
 - (1) The current body of enumerated Common Vulnerabilities and Exposures (CVE), Common Configuration Enumerations (CCE), and Common Platform Enumerations (CPE);
 - (2) The full list of vendor-released patches for supported hardware and software assets; and
 - (3) Checklists from the NIST *National Checklist Program* ([NCP](#)) Repository or other authoritative baseline security configuration guidelines, in accordance with DR 3520-002.
- l. Mission Areas, agencies, and staff offices will:
 - (1) Ensure that their monthly vulnerability scans include all hardware and software assets;
 - (2) Identify and document all false positive findings or other discrepancies from Department vulnerability scans; and
 - (3) Provide required monthly vulnerability scan artifacts to ISC via email to ISC.Outreach@wdc.usda.gov.
- m. All hardware and software assets on all USDA information systems will be scanned for vulnerabilities each month, or more frequently, such as:
 - (1) When stated in the System Security Plan (SSP);
 - (2) When directed because of an elevated risk level;
 - (3) After installation, modification, or update of software or hardware;
 - (4) After a configuration change; or

- (5) When conducting validation scans.
- n. Written justification will be provided for any modification to the Common Vulnerability Scoring System (CVSS) or Common Configuration Scoring System (CCSS) scoring methods or adjustment to the scores associated with the vulnerability severity levels and obtain approval from the Mission Area Assistant Chief Information Security Officer (CISO) or Information System Security Program Manager (ISSPM) for these changes.
 - o. All critical vulnerability findings will be remediated within 14 days or in the timeframe indicated by the USDA CISO or designated authority.
 - p. All vulnerabilities rated as high, moderate, or low risk will be remediated within 30 days or have a POA&M created and managed in the Department's official system of record in accordance with [DR 3565-003](#), *Plan of Action and Milestones Policy*.
 - q. Critical vulnerabilities identified in the Department of Homeland Security (DHS) Binding Operational Directive (BOD) Cyber Hygiene reports that are not remediated within 30 days, will be documented in a memorandum. The memorandum will adhere to the guidance in the applicable BOD, explain or justify the delay, be signed by the responsible Administrator and the Mission Area Assistant Chief Information Officer (CIO), and be submitted to the Secretary of Agriculture through the USDA CISO and USDA CIO.
 - r. All ISC Alerts addressing emergency patches will be implemented within the required timeframe in accordance with the direction from the USDA CISO or the United States Computer Emergency Readiness Team (US-CERT). Documentation demonstrating when and what actions were taken will be submitted via email to ISC.Outreach@wdc.usda.gov.
 - s. Sufficient resources will be applied to expeditiously resolve all ISC Alerts addressing zero-day exploits, regardless of severity level.
 - t. Vulnerability scans will be performed on all new, upgraded, or modified hardware and software as part of the security assessment process, before introduction into an operational environment. Mission Areas, agencies, and staff offices will:
 - (1) Remediate all critical and high findings prior to being installed or reinstalled (in the case of upgraded or modified systems) into the operational environment; and
 - (2) Enter POA&Ms into the Department's FISMA data management and reporting tool for all moderate and low severity vulnerability findings that cannot be remediated prior to introduction into the production environment.
 - u. Waivers will be requested for:
 - (1) Any vulnerability finding that either cannot be remediated, will not be remediated in the timeframe required or committed to, or requires considerably more resources for remediation than the assessed risk warrants;

- (2) Exceptions to, or deviations from, required security configuration baselines;
 - (3) Any software update or hardware upgrade that has an unmitigated critical or high vulnerability finding, before being introduced into an operational environment; or
 - (4) Access to, or use of, a restricted or prohibited device, system, software application.
- v. Patches will only be downloaded from trusted sources, their authenticity validated through methods such as digital signatures, digital certificates, or checksums, and scanned for malware.
 - w. All patches and other vulnerability remediation measures (e.g., fixing misconfigurations, closing ports, disabling unnecessary protocols or services) will be implemented adhering to Mission Area, agency, or staff office configuration change control processes.
 - x. Only personnel with appropriate training and qualifications will be authorized to implement hardening actions or install patches on systems.
 - y. Validation scans will be conducted on systems after vulnerability patches or remediation changes have been applied to ensure that the vulnerabilities have been remediated and no new vulnerabilities have been introduced during the remediation process.
 - z. Mission Areas, agencies, and staff offices will collaborate with ISC to provide additional information, as needed, to reconcile false positive findings or differences in scan output, or other information related to scan vulnerabilities or mitigations.
 - aa. Monthly inventory, configuration, and patch vulnerability scan reports will be retained in encrypted format for 1 year.
 - bb. Requirements to scan for and remediate configuration and patch vulnerabilities on interconnected systems will be incorporated into interconnection security agreements (ISA), MOUs, or memoranda of agreement (MOA).

6. ROLES AND RESPONSIBILITIES

- a. The USDA CIO will:
 - (1) Ensure the USDA information security program addresses inventory, configuration, and patch vulnerability scanning and remediation activities, as well as FISMA compliance and other Federal requirements, including risk mitigation requirements;
 - (2) Ensure funding for the Department-level program, resources, and capabilities for inventory, configuration, and patch vulnerability scanning and remediation; and
 - (3) Ensure that required data and other relevant metrics for inventory, configuration, and patch vulnerability scanning and remediation are regularly collected, analyzed, and reported.

b. The USDA CISO will:

- (1) Ensure the development, implementation, and maintenance of the Departmental inventory, configuration, and patch vulnerability scanning and remediation program, policies, and associated procedures;
- (2) Disseminate guidance for inventory, configuration, and patch vulnerability scanning and remediation to Mission Area Assistant CIOs, as well as Mission Area Assistant CISOs and Mission Area, agency, and staff office ISSPMs;
- (3) Ensure that ISC develops, effectively implements, and maintains documented procedures for all inventory, configuration, and patch vulnerability scanning and remediation activities and capabilities;
- (4) Ensure that ISC personnel that support the inventory, configuration, and patch vulnerability scanning and remediation program are trained on applicable policies and procedures, as well as associated requirements, standards, and guidelines issued by OMB, DHS, NIST, and USDA;
- (5) Ensure that ISC implements required capabilities, tools, processes, and procedures to gather data and relevant metrics on inventory, configuration, and patch vulnerability scanning and remediation, and meets all Departmental reporting requirements;
- (6) Ensure that relevant data and metrics for inventory, configuration, and patch vulnerability scanning and remediation are regularly collected, analyzed, reported, and used to continuously improve Departmental information security;
- (7) Ensure sufficient funding is allocated to maintain the effectiveness of the inventory, configuration, and patch vulnerability scanning and remediation program, including role-based training for ISC personnel supporting the program;
- (8) Notify Mission Areas, agencies, and staff offices of any identified critical vulnerabilities requiring emergency patch or remediation actions outside of the monthly scanning and reporting cycle;
- (9) Ensure Mission Areas, agencies, and staff offices submit monthly scan artifacts and updates to inventory, vulnerability, and POA&M management databases, and comply with other related oversight requirements;
- (10) Ensure that ISC personnel conduct compliance reviews on a representative sample of monthly scan and patch result submissions and that corrective actions are taken on identified vulnerabilities within the required timeframes;
- (11) Ensure that ISC personnel disseminate reports and analyses to the relevant organizations and work with identified points of contact to resolve discrepancies in the reports;

- (12) Ensure development and maintenance of:
 - (a) The USDA inventory of high value assets (HVA) and public-facing IP address ranges related to those assets; and
 - (b) Automated methods and procedures for reporting this information to DHS.
- (13) Review and sign each request for waiver, indicating its disposition with a comment;
- (14) Track Departmental compliance with inventory, configuration, and patch vulnerability scanning and remediation requirements and provide compliance reports to the USDA CIO; and
- (15) Ensure the Departmental President's Management Council (PMC) reports include all critical DHS BOD Cyber Hygiene vulnerabilities not remediated within 30 days.
- c. Agency Administrators and Staff Office Directors will submit memoranda to the Secretary of Agriculture, through the Mission Area Assistant CIO, the USDA CISO, and the USDA CIO, documenting critical vulnerabilities identified in DHS BOD Cyber Hygiene reports that are not remediated within 30 days.
- d. AOs will review and either approve or deny waivers and exceptions to policy related to systems under their purview. Waiver approval authority cannot be delegated.
- e. Mission Area Assistant CIOs will:
 - (1) Fund and ensure development, effective implementation, and maintenance of procedures, resources, and capabilities for inventory, configuration, and patch vulnerability scanning and remediation for their area of responsibility;
 - (2) Ensure that personnel responsible for inventory, configuration, and patch vulnerability scanning and remediation receive annual role-based training, maintain qualifications, and are authorized to conduct these activities;
 - (3) Provide direction to Mission Area, agency, and staff office personnel to comply with Federal and Departmental regulations, requirements, and standards for inventory, configuration, and patch vulnerability scanning and remediation;
 - (4) Ensure that their organization develops, documents, implements, reviews, and updates procedures for inventory, configuration, and patch vulnerability scanning and remediation that align with Federal and Departmental requirements;
 - (5) Ensure coordination between:
 - (a) Scanning and vulnerability management activities;
 - (b) Inventory management requirements; and
 - (c) Configuration management and change control processes.

- (6) Ensure that personnel in their area of responsibility cooperate with ISC and provide all requested information and artifacts in a timely manner; and
 - (7) Ensure accurate inventory, configuration, and patch information is provided to ISC each month.
- f. Mission Area Assistant CISOs, and Mission Area, Agency, and Staff Office ISSPMs will:
- (1) Disseminate this policy and any accompanying procedures to personnel responsible for inventory, configuration, and patch vulnerability scanning and remediation;
 - (2) Ensure that Mission Area, agency, and staff office procedures for inventory, configuration, and patch vulnerability scanning and remediation are developed, documented, implemented, and maintained for their area of responsibility;
 - (3) Ensure that this policy and any accompanying procedures are effectively implemented and integrated within their area of responsibility;
 - (4) Ensure that ISAs, MOUs, or MOAs for interconnected systems include requirements for inventory, configuration, and patch vulnerability scanning and remediation;
 - (5) Ensure that personnel assigned responsibilities for inventory, configuration, and patch vulnerability scanning and remediation are trained;
 - (6) Ensure that monthly scans are performed in accordance with Departmental inventory, configuration, and patch vulnerability scanning and remediation requirements;
 - (7) Review and either approve or deny requests to:
 - (a) Perform external scans; or
 - (b) Modify the CVSS scoring method to prioritize remediation activities based on impact to the organization.
 - (8) Ensure that false positive findings from inventory and vulnerability scans are identified and reported to ISC with explanations for the false positive findings;
 - (9) Report all critical vulnerabilities within required timeframes to the Mission Area Assistant CIO and others, according to Departmental guidance;
 - (10) Ensure that all required inventory, configuration, and patch:
 - (a) Scans results are submitted to ISC monthly via ISC.Outreach@wdc.usda.gov; and
 - (b) POA&Ms are submitted and discrepancies reconciled each month with ISC.

- (11) Ensure that missing and incorrect inventory values and vulnerability discrepancies reported by ISC are promptly resolved;
- (12) Ensure Mission Area, agency, or staff office inventory of HVAs and public-facing IP addresses or IP ranges for those assets are correlated and provided to USDA CISO;
- (13) Ensure that findings from both USDA monthly vulnerability scans and the DHS BOD Cyber Hygiene report are remediated within the mandated timeframes;
- (14) Ensure POA&Ms for vulnerabilities that are not remediated within 30 days are entered into the FISMA data management and reporting tool and managed to closure;
- (15) Ensure that waiver requests with strong justification are submitted to the AO for all vulnerability findings when remediation activities are not or cannot be undertaken;
- (16) Ensure the monthly inventory, configuration, and patch vulnerability scan reports are encrypted and archived for 1 year; and
- (17) Ensure appropriate staff subscribe to receive information about threats, vulnerabilities, and remediation strategies from trusted resources, such as:
 - (a) [*US-CERT Alerts*](#);
 - (b) [*US-CERT Bulletins*](#);
 - (c) [*US-CERT Current Activity*](#);
 - (d) Carnegie Mellon University, [*Vulnerability Notes Database*](#); and
 - (e) Vendor security and patching information.

g. System Owners will:

- (1) Request funding to support inventory, configuration, and patch vulnerability scanning and remediation activities;
- (2) Ensure the SSP includes required inventory, configuration, and patch vulnerability scanning and remediation activities;
- (3) Ensure monthly inventory, configuration, and patch vulnerability scans are performed and that the scanning tools are properly updated with CVE, patch, and other current information prior to performing the scans;
- (4) Ensure monthly inventory scan information is reconciled with the Departmental inventory and sent to ISC via ISC.Outreach@wdc.usda.gov;

- (5) Ensure vulnerabilities are mitigated for all components of the system in accordance with priorities and required timeframes;
- (6) Ensure configuration change control processes are followed for applying patches and remediating other vulnerabilities;
- (7) Prepare and submit waiver requests to the Mission Area Assistant CISO or the Mission Area, agency, or staff office ISSPM for review and forwarding to the AO for approval;
- (8) Ensure the monthly scan and remediation artifacts are submitted to ISC and the Mission Area Assistant CISO or Mission Area, agency, or staff office ISSPM when required;
- (9) Prepare a memorandum for any critical vulnerability identified in the DHS BOD Cyber Hygiene scan which cannot be remediated within 30 days;
- (10) Ensure personnel collaborate with ISC analysts to resolve discrepancies between Departmental and Mission Area, agency, and staff office inventory or vulnerability findings;
- (11) Ensure that any downloaded patches are validated for authenticity and scanned for malware before testing or installing them;
- (12) Ensure patch installations and other vulnerability fixes (e.g., correcting misconfigurations, hardening) are performed in compliance with change control and remediation testing processes; and
- (13) Ensure personnel take annual role-based training related to their inventory, configuration, and patch vulnerability scanning and remediation responsibilities.

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.
- 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 Mission Areas, agencies, and staff offices are required to conform to this policy. If a specific policy requirement cannot be met as explicitly stated, a waiver may be requested. Note that an approved waiver does not bring the system into compliance with policy. Requests for waivers:
 - (1) Are an acknowledgement of a system's non-compliance with policy and that an acceptable plan to remediate the weakness has been provided and will be implemented.
 - (2) Must be documented as indicated in CAPE-SOP-003.
- 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 OCIO Information Security Center via email to the csc@ocio.usda.gov mailbox.

-END-

APPENDIX A

AUTHORITIES AND REFERENCES

Carnegie Mellon University, Software Engineering Institute, [Vulnerability Notes Database](#)

CNSS, [CNSS Instruction No. 4009](#), *Committee on National Information Assurance (CNSS) Glossary*, April 6, 2015

DHS, [FY 2018 CIO FISMA Metrics](#), Version 2.0, April 2018

Federal Information Security Modernization Act of 2014, ([FISMA](#)), 44 U.S.C. § 3541, et seq.

GSA, Federal Risk and Authorization Management Program (FedRAMP), [Guide to Understanding FedRAMP](#), version 1.2, April 22, 2013

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

NIST, [IR 7435](#), *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems*, August 2007

NIST, [IR 7502](#), *The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities*, December 2010

NIST, [IR 7511 Revision 4](#), *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*, January 2016

NIST, [IR 7946](#), *CVSS Implementation Guidance*, April 2014

NIST, [National Checklist Program Repository](#)

NIST, [National Vulnerability Database](#)

NIST, [SP 800-40 Revision 3](#), *Guide to Enterprise Patch Management Technologies*, July 2013

NIST, [SP 800-51 Revision 1](#), *Guide to Using Vulnerability Naming Schemes*, February 2011

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 800-115](#), *Technical Guide to Information Security Testing and Assessment*, September 2008

NIST, [SP 800-126 Revision 3](#), *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2*, February 2018

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

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

Office of Government Ethics, [Standards of Ethical Conduct for Federal Employees of the Executive Branch](#), 5 Code of Federal Regulations §2635, et seq., (2018)

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

OMB, Memorandum [M-14-03](#), *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013

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

OMB, Memorandum [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, [DM 3530-004](#), *Firewall Technical Security Standards*, February 17, 2005

USDA, [DR 3520-002](#), *Configuration Management*, August 12, 2014

USDA, [DR 3565-003](#), *Plan of Action and Milestones Policy*, September 25, 2013

USDA, [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, October 4, 2007

US-CERT, [US-CERT Alerts](#)

US-CERT, [US-CERT Bulletins](#)

US-CERT, [US-CERT Current Activity](#)

APPENDIX B

DEFINITIONS

Common Configuration Enumeration (CCE). A nomenclature and dictionary of software security configurations. (Source: NIST SP 800-126 Revision 2)

Common Configuration Scoring System (CCSS). A set of measures of the severity of software security configuration issues. (Source: NIST IR 7502)

Common Platform Enumeration (CPE). A nomenclature and dictionary of hardware, operating systems, and applications. (Source: NIST SP 800-126 Revision 2)

Common Vulnerabilities and Exposures (CVE). A nomenclature and dictionary of security-related software flaws. (Source: NIST SP 800-126 Revision 2)

Common Vulnerability Scoring System (CVSS). An SCAP specification for communicating the characteristics of vulnerabilities and measuring their relative severity. (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 800-53 Revision 4)

Configuration Management. A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle. (Source: NIST SP 800-53 Revision 4)

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)

Credentialed Scan. Also referred to as an authenticated scan. Scans that use login identifiers and user roles (e.g., root, administrator) that offer the greatest possible privileges for the system being scanned. (Source: Adapted from FedRAMP (Federal Risk and Authorization Management Program), *Guide to Understanding FedRAMP*, version 1.2, April 22, 2013)

Enumeration. A standard nomenclature (naming format) and an official dictionary or list of items, such as products (platforms), software security configurations, or security-related software flaws, used by SCAP. (Source: Adapted from NIST SP 800-117 Revision 1)

Hardening. Configuring a host's operating systems and applications to reduce the host's security weaknesses. (Source: NIST IR 7298 Revision 2)

High Value Assets. Those assets, Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or state-sponsored actors for either direct exploitation or to cause a loss of confidence in the U.S. Government. (Source: OMB Memorandum M-17-09)

Misconfiguration. A setting within a computer program that violates a configuration policy or that permits or causes unintended behavior that impacts the security posture of a system. CCE can be used for enumerating misconfigurations. (Source: NIST IR 7511 Revision 4)

National Checklist Program (NCP) Repository. A NIST maintained repository, which is a publicly available resource that contains information on a variety of security configuration checklists for specific information technology products or categories of products. (Source: NIST IR 7511 Revision 4)

Organization. An entity of any size, complexity, or positioning within an organizational structure (e.g., federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements). (Source: NIST SP 800-37 revision 2)

Patch. An update to an operating system, application, or other software issued specifically to correct particular problems with the software. (Source: NIST IR 7298 Revision 2)

Patch Management. Systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. (Source: CNSS Instruction No. 4009)

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 SP 800-40 Revision 3)

Security Content Automation Protocol (SCAP). A method for using specific standardized testing methods to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements. (Source: CNSS Instruction No. 4009)

USDA employee. A Federal civil servant employed by, detailed or assigned to, USDA, including members of the Armed Forces.

USDA Personnel. USDA employees, contractors, affiliates, interns, fellows, and volunteers who work for, or on behalf of, USDA, and whose work is overseen by USDA employees.

Vulnerability. Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (Source: NIST SP 800-53 Revision 4)

Vulnerability Scanning. A technique used to identify hosts/host attributes and associated vulnerabilities. (Source: NIST SP 800-115)

APPENDIX C

ACRONYMS AND ABBREVIATIONS

AO	Authorizing Official
ASOC	Agriculture Security Operations Center
ASOD	Agriculture Security Operations Division
BOD	Binding Operational Directive
CCE	Common Configuration Enumeration
CCSS	Common Configuration Scoring System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
COTS	Commercial Off-the-Shelf
CPE	Common Platform Enumeration
CSIP	Cybersecurity Strategy and Implementation Plan
CSIRT	Cybersecurity Incident Response Team
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DM	Departmental Manual
DR	Departmental Regulation
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act
HVA	High Value Asset
IP	Internet Protocol
IR	Interagency Report
ISA	Interconnection Security Agreement
ISC	Information Security Center
ISSPM	Information Systems Security Program Manager
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCP	National Checklist Program
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PMC	President's Management Council
POA&M	Plan of Action and Milestones
SCAP	Security Content Automation Protocol
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
US-CERT	United States Computer Emergency Readiness Team
USDA	United States Department of Agriculture
USGCB	United States Government Configuration Baseline
U.S.C.	United States Code

VoIP Voice over Internet Protocol