

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

DEPARTMENTAL REGULATION	NUMBER: DR 3575-002
SUBJECT: System and Information Integrity	DATE: August 16, 2018
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: August 16, 2023

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Scope	2
3. Special Instructions/Cancellations	3
4. Background	3
5. Policy	4
6. Roles and Responsibilities	9
7. Penalties and Disciplinary Actions for Non-Compliance	13
8. Policy Exceptions	13
9. Inquiries	13
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 for system and information integrity.
- b. It is the policy of USDA to comply with Federal requirements to establish, implement, and enforce a system and information integrity policy to continually manage risks to USDA information resources.
- c. This policy complies with the requirements of the *Federal Information Security Modernization Act of 2014* ([FISMA](#)); Federal Information Processing Standards Publication ([FIPS PUB](#)) [200](#), *Minimum Security Requirements for Federal Information and Information Systems*; and 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*.

- d. This policy serves as the foundation on which agencies and staff offices are to develop, implement, and maintain system and information integrity procedures that comply with Federal and Departmental requirements.

2. SCOPE

- a. This policy applies to all USDA Mission Areas, agencies, staff offices, employees, appointees, contractors, and others who work for or on behalf of USDA and are responsible for system and information integrity at any phase in the system life cycle, whether during acquisition and development, implementation, operations and usage, or system disposition.
- b. This policy also applies to:
 - (1) All Federal information, in any medium or form, generated, collected, provided, transmitted, stored, maintained, or accessed by or on behalf of USDA; and
 - (2) Information systems or services (including cloud-based services) used or operated by USDA, USDA contractors, subcontractors, or other organizations on behalf of or funded by USDA, and interconnections between or among systems or services.
- c. This policy complements other Departmental policies that cover similar topics, but this DR is written from the information security perspective of the NIST system and information integrity control family. The complementary aspects of this policy address monitoring for unauthorized access to Web sites or use of USDA's information resources that constitute actual and suspected security violations. Complementary policies include:
 - (1) [DR 1495-001](#), *New Media Roles, Responsibilities and Authorities*;
 - (2) [DR 3300-001](#), *Telecommunications & Internet Services and Use*; and
 - (3) [Department Manual \(DM\) 3300-005](#), *Policies for Planning and Managing Wireless Technologies in USDA*.
- d. This document is closely related to the following DRs, DMs, and standard operating procedures (SOPs):
 - (1) [DM 3530-001](#), *USDA Vulnerability Scan Procedures*;
 - (2) [DM 3535-002](#), *Chapter 7, Part 2 Patch Management and Systems Updates*;
 - (3) [DR 3520-002](#), *Configuration Management*;
 - (4) [DR 3505-005](#), *Cyber Security Incident Management Policy*; and

- (5) Information Security Center (ISC), (formerly the Compliance, Audit, Policy, and Enforcement (CAPE) Division), [CAPE-SOP-004](#), *USDA Six-Step Risk Management Framework (RMF) Process Guide*.
- e. Nothing in this policy shall alter the requirements for the protection of information associated with national security systems such as those in FISMA, policies, directives, instructions, or standards issued by the Committee on National Security Systems (CNSS) or intelligence community.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy is effective immediately when published and will remain in effect until superseded.
- b. The term “agency” or phrase “agency and staff office,” unless otherwise noted in this document, will be considered to encompass the Mission Areas, agencies, and staff offices of USDA.
- c. All agencies and staff offices shall align their policies and procedures with this DR within 6 months of the publication date.
- d. In this document, the terms:
 - (1) “Low,” “moderate,” and “high” impact categories refer to the three levels of potential impact on organizations or individuals in the event of a security breach (i.e., loss of confidentiality, integrity, or availability) of systems, as designated under NIST, [FIPS PUB 199](#), *Standards for Security Categorization of Federal Information and Information Systems*;
 - (2) “Software” is used to encompass types of software such as 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 by vendors into hardware appliances to perform tasks such as big data analytics or intrusion protection. “Firmware” may be mentioned separately from “software;” and
 - (3) “Vulnerability” is used instead of “flaw” to describe weaknesses in systems or protection mechanisms that must be remediated.

4. BACKGROUND

While existing information security DRs address specific technical techniques to prevent malicious acts, achieving system and information integrity requires full life cycle and defense-in-depth strategies. Early in the life cycle, requirements for system and information integrity must be documented and incorporated into statements of work (SOWs) and

contracts for information technology (IT) products and for services, such as software development, systems integration, and cloud-based services. Security controls appropriate to the system categorization level must be implemented as part of development. Vulnerabilities must be identified and remediated in both the development and operations and maintenance phases of the life cycle. Automated monitoring during operations helps detect unauthorized activities that may impact not just the integrity of systems and information but also confidentiality and availability.

Defense-in-depth strategies apply to all components of a system, from workstations and other end devices to servers, appliances, and network equipment. The defense-in-depth strategies must integrate elements such as configuration management; system auditing practices; security assessments; and protections against malicious code, spam, phishing, and other types of attacks, intrusion detection, and prevention mechanisms.

The timely manner in which vulnerabilities are mitigated is based on several factors such as agency or staff office resources, its processes to approve and implement corrective action, the impact of an exploited vulnerability, and the conditions required to exploit the vulnerability.

5. POLICY

- a. Agencies and staff offices shall establish, implement, and maintain system and information integrity policies and procedures to include:
 - (1) Robust integration of system and information integrity processes throughout the life cycle activities of all information systems and services used or operated by or on behalf of USDA; and
 - (2) Integration with other processes such as risk assessment and risk management; configuration management; security assessments; continuous monitoring; incident management; auditing; and scanning and remediation of configuration and patch vulnerabilities.
- b. System and information integrity requirements shall be included in all SOWs and procurement requests for all contracts involving acquisition of:
 - (1) COTS and open source software;
 - (2) Custom development or maintenance of software;
 - (3) System integration services, both initial integration and maintenance of operational systems; and
 - (4) Cloud-based services.
- c. Agencies and staff offices with a high impact categorization information system or service that uses binary or machine-executable code from sources with no warranty shall:

- (1) Submit exception requests to ISC.outreach@wdc.usda.gov, unless the accompanying source code has been provided for security and vulnerability testing;
 - (2) Only implement and maintain the system or service under an approved exception request and with compensating controls appropriate to the assessed level of risk; and
 - (3) Document compensating controls in the security plan.
- d. Agencies and staff offices shall, for all information systems and services:
- (1) Incorporate vulnerability remediation into processes for:
 - (a) Configuration management; and
 - (b) Scanning and remediation of configuration and patch vulnerabilities.
 - (2) Rigorously test for vulnerabilities using documented test plans or procedures before installation into operational environments;
 - (3) Document findings of software and information system vulnerabilities; and
 - (4) Correct vulnerabilities in a timely manner.
- e. Agencies and staff offices that have one or more information system or service with a moderate or high impact categorization shall implement and run automated mechanisms, at least monthly, to determine the state of system components with respect to weaknesses and vulnerabilities (e.g., patches, service packs, malware signatures) as part of the vulnerability remediation process.
- f. Agencies and staff offices that have one or more information system or service with a high impact categorization shall implement a centrally managed vulnerability remediation process that encompasses activities such as planning, implementing, assessing, authorizing, and monitoring the security controls for vulnerability remediation.
- g. Agencies and staff offices shall protect their systems (including workstations, mobile devices, and servers) from malicious code by ensuring that:
- (1) All systems employ malicious code protection mechanisms at all times to detect and eradicate malicious code prior to its execution, no matter the method of exposure (e.g., Web access, email, email attachments, removable media);
 - (2) Malicious code protection mechanisms are updated whenever new releases are available;
 - (3) Users receive guidance when to apply or not apply malicious code protection to their devices; and

- (4) Information systems and services with a moderate or high impact categorization:
 - (a) Automatically update malicious code protection mechanisms;
 - (b) Employ centralized management processes for planning, implementing, assessing, authorizing, and monitoring the malicious code protection mechanisms; and
 - (c) Integrate malicious code protection mechanisms with auditing processes to log the detection of malicious code as an event.
- h. Agencies and staff offices shall protect their information systems and services from spam, phishing, and other malicious tactics, techniques, and procedures by ensuring that:
 - (1) Layered protection mechanisms are employed at system entry and exit points to detect and take action on unsolicited messages;
 - (2) Protection mechanisms are updated whenever new releases are available; and
 - (3) Information systems and services with a moderate or high impact categorization:
 - (a) Automatically update protection mechanisms; and
 - (b) Employ centralized management processes for planning, implementing, assessing, authorizing, and monitoring the protection mechanisms.
- i. Anti-spam and anti-phishing detection systems shall include and implement techniques to reduce false positives and false negatives.
- j. Agencies and staff offices shall assign their own personnel or contract with a third party (contractor) to ensure that all information systems and services are monitored continuously with automated devices in order to:
 - (1) Detect attacks or indicators of potential attacks;
 - (2) Detect unauthorized local, network, and remote connections; and
 - (3) Identify unauthorized system use.
- k. Agencies and staff offices shall have a governing document (e.g., contract, memorandum of understanding, memorandum of agreement, service level agreement) to ensure metadata, log files, configurations, and all security-related information needed to verify compliance with Departmental information and information system integrity requirements are provided to USDA personnel or personnel acting for or on behalf of USDA.
- l. Access to the Web-based services or applications identified in Section 5m shall be denied in accordance with [DM 3530-004](#), *Firewall Technical Standards* unless the USDA Chief Information Security Officer (CISO) approves a waiver.

- m. The following types of Web-based services or applications shall be monitored; unauthorized user access or use of them from a USDA system or device shall be considered a security violation:
 - (1) Unauthorized file sharing and file hosting sites;
 - (2) Unauthorized streaming services (e.g., Pandora, Netflix);
 - (3) Gambling sites including those for poker games and fantasy sports; and
 - (4) Sites hosting or promoting illegal or offensive content (e.g., terrorism, hate crimes, sexually explicit material) or illegal activities (e.g., sale or trafficking of stolen goods).
- n. Agencies and staff offices that have information systems and services with a moderate or high impact categorization shall ensure that inbound and outbound communications traffic is monitored for unusual or unauthorized activities or conditions and that this monitoring capability is either self-provisioned or outsourced.
- o. Agencies and staff offices that have information systems and services with a moderate or high impact categorization shall ensure that the monitoring of those systems, whether self-provisioned or outsourced:
 - (1) Is performed with automated tools that support near real-time analysis of events; and
 - (2) Provides alerts of indicators of compromise or potential compromise from sources such as audit records, malicious code protection mechanisms, intrusion detection or prevention mechanisms, or firewalls notifying personnel identified in the security plan.
- p. Agencies and staff offices that have information systems and services with a moderate or high impact categorization shall:
 - (1) Determine which error conditions should be identified, rank the priorities for handling them based on an assessment of risk, and then document this information;
 - (2) Design and implement the systems to generate and log error messages, as part of the audit record, to provide information necessary for corrective actions without revealing information that could be exploited by adversaries;
 - (3) Ensure that the systems are configured to reveal error messages only to authorized personnel;
 - (4) Ensure that the systems implement safeguards to protect memory from unauthorized code execution;
 - (5) Ensure that the systems are designed and implemented to:

- (a) Check information system inputs (i.e., syntax and semantics) for accuracy, completeness, and validity performing the checks as close to the input point (e.g., user interface) as possible; and
 - (b) Verify that the inputs match specified definitions for format and content.
- (6) Employ integrity verification tools to detect unauthorized changes to sensitive information and software; and
- (7) Incorporate the detection of unauthorized, security-relevant changes into their incident response and incident management capabilities.
- q. Agencies and staff offices that have information systems and services with a high impact categorization shall ensure that the systems are designed and implemented to:
 - (1) Verify the correct operation of security functions;
 - (2) Perform the verification and respond when anomalies are discovered, as documented in the system security plan; and
 - (3) Notify responsible personnel of failed security verification tests.
- r. Agencies and staff offices that have information systems and services with a high impact categorization shall:
 - (1) Employ tools that provide automated notifications to responsible personnel upon discovery of discrepancies in or violations of integrity;
 - (2) Ensure that the systems respond automatically when integrity violations are discovered;
 - (3) Prohibit the use of binary or machine-executable code from sources with no warranty, unless source code is provided and rigorously tested for malicious code and vulnerabilities; and
 - (4) Request exceptions to the source code requirement only for compelling mission-related requirements, and obtain the written approval of the authorizing official and the USDA CISO.
- s. Agencies and staff offices shall:
 - (1) Disseminate security alerts, advisories, and directives to personnel within the organization who have a need to know or have responsibilities to implement the directives; and
 - (2) Ensure that each security directive is properly implemented in accordance with established timeframes, and, if not implemented, notify the Departmental issuer or transmitter of the directive regarding the degree of noncompliance.

- t. Agencies and staff offices shall handle and retain information within their information systems and hardcopy and electronic information outputs from those systems throughout all phases of the system life cycle in accordance with applicable Federal and Departmental requirements, to include records management requirements.
- u. Agencies and staff offices shall establish and enforce procedures to ensure that sensitive information within their systems and the information outputs from those systems cannot be accessed or stolen by unauthorized individuals.

6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) shall:
 - (1) Delegate the authority to the USDA CISO to ensure that acquisitions of IT products (e.g., hardware or software) and services (such as software development and systems integration) adequately address Federal and Departmental requirements for systems and information integrity; and
 - (2) Manage USDA's records management program to ensure that information within information systems and information outputs from systems are handled and retained in accordance with applicable Federal and Departmental requirements.
- b. The USDA CISO shall:
 - (1) Coordinate with and provide guidance to agency and staff office CISOs and Information Systems Security Program Managers (ISSPMs) on compliance with Federal and Departmental system and information integrity requirements;
 - (2) Provide oversight of agency and staff office information security programs to ensure implementation of this policy and compliance with Federal and Departmental system and information integrity requirements, including: integration with system life cycle management; risk assessment and risk management; security assessments; plans of action and milestones (POA&Ms) and waiver requests; configuration management; and scanning and remediation of configuration and patch vulnerabilities;
 - (3) Ensure that acquisitions of IT products (e.g., hardware, software) and services (e.g., cloud-based systems, software development, systems integration) adequately address Federal and Departmental system and information integrity requirements;
 - (4) Provide and manage enterprise protection against threats such as malicious code, spam, and phishing attacks at the enterprise entry and exit points;
 - (5) Monitor and log unauthorized use or activity such as access to prohibited Web sites and file downloads, and when feasible, block unauthorized network traffic at the enterprise entry and exit points;

- (6) Offer managed information system monitoring services to agencies and staff offices;
 - (7) Provide enterprise security solutions such as spam, phishing, and malware protection or offer contractual vehicles for such solutions;
 - (8) Generate and distribute security alerts, advisories, and directives and ensure timely follow-up on actions required by directives; and
 - (9) Ensure that user awareness training includes techniques for recognizing and properly responding to occurrences of spam, phishing attacks, and malicious code.
- c. Mission Area Assistant CIOs shall:
- (1) Hold agency and staff office personnel accountable for complying with Federal and Departmental system and information integrity requirements; and
 - (2) Provide adequate budget funding for malicious code, spam, and phishing attack protection mechanisms and qualified staff to manage the associated processes.
- d. Authorizing Officials shall:
- (1) Be responsible for risk-based decisions regarding system and information integrity; and
 - (2) Adjudicate requests for waivers from requirements that prohibit use of binary or machine executable code from sources with no warranty and without the provision of source code, and approve these only for compelling mission and operational requirements.
- e. Agency Contracting Officers shall ensure the documents governing the relationship between USDA and service providers define the expectations of performance for each required information and information system integrity security control, describe measurable outcomes, and identify remedies and response requirements for any identified instances of non-compliance with Departmental information and information system integrity requirements are provided to USDA personnel or to others as directed by USDA personnel.
- f. System Owners shall ensure the following throughout the system life cycle:
- (1) Vulnerability remediation processes are implemented and integrated with configuration management processes;
 - (2) Malicious code protection mechanisms are implemented effectively and broadly (e.g., prior to installation and post-installation of media storage or software);
 - (3) Mail and messaging systems are protected from spam, phishing, and other types of attacks, and the system plans document the deployed mechanisms;

- (4) Monitoring is employed to detect attacks or indicators of potential attacks and unauthorized connections, accesses, and downloads and integration with incident management processes;
- (5) Systems are protected by integrity verification mechanisms, which are documented in the security plans, to detect unauthorized changes, and processes are in place to respond to notifications of discrepancies during integrity verification;
- (6) Systems are designed to check for valid syntax and semantics of inputs and are implemented to verify that inputs match the specified definitions, as documented in the system design document or security plan;
- (7) Systems are designed and implemented in accordance with information security practices for handling errors and generating error messages, and the system documentation or security plan documents these capabilities; and
- (8) Information within information systems and information outputs from systems are handled and retained in accordance with applicable Federal and Departmental requirements;
- (9) For high impact systems:
 - (a) Ensure that automatic protections respond appropriately when integrity violations are detected and that the selected response mechanisms are documented in the security plans;
 - (b) Ensure that these systems do not contain binary or machine-executable code from sources with no warranty unless the source code has been provided and tested for vulnerabilities and malformed code or unless the authorizing official and the USDA CISO approve a waiver from this requirement; and
 - (c) Ensure these systems are designed and implemented to protect memory from unauthorized code execution, with the methods for accomplishing this documented in the system documentation or security plan.

g. Agency and Staff Office CISOs and ISSPMs shall:

- (1) Ensure that information systems and services are well monitored (especially when notified of increased threats) to detect attacks, indicators of potential attacks, and unauthorized connections, accesses, and downloads;
- (2) Ensure that there is integration between monitoring procedures and the documented incident management procedures;
- (3) Ensure that information systems and services implement malicious code, spam, and phishing attack protection mechanisms;

- (4) Ensure that role-based training for network and system administrators includes procedures for installing, operating, and updating malicious code, spam, and phishing attack protection mechanisms;
 - (5) Ensure that robust vulnerability remediation processes are in place and integrated with processes for configuration management and for scanning and remediation of vulnerabilities;
 - (6) Provide guidance to system owners on system and information integrity requirements and techniques and tools for satisfying those requirements;
 - (7) Provide oversight and guidance when security alerts, advisories, and directives are issued, and ensure that security directives are implemented in accordance with established timeframes or notify the issuer of the degree of noncompliance; and
 - (8) Provide guidance and oversight to system owners and users to ensure that information within information systems and information outputs from systems are handled and retained in accordance with applicable Federal and Departmental requirements.
- h. System Administrators shall:
- (1) Securely deploy, maintain, and administer systems using appropriate malicious code protection mechanisms and ensure the protection mechanisms are regularly updated;
 - (2) Securely deploy, maintain, and administer mail and other messaging servers so that they are protected from spam, phishing, and other types of attacks following NIST guidelines, and ensure the anti-spam and anti-phishing protection mechanisms are regularly updated;
 - (3) Ensure that mail and messaging client systems are securely deployed, maintained, and administered to protect them from spam, phishing, or other types of attacks; and
 - (4) Implement and maintain integrity verification mechanisms to detect unauthorized changes to information systems, and follow documented processes when there are notifications of discrepancies discovered during integrity verification.
- i. All users shall:
- (1) Properly handle and protect information outputs in all formats, whether digital (such as on discs or flash drives) or non-electronic (such as printouts) in accordance with applicable Federal and Departmental requirements; and
 - (2) Follow Department, agency, or staff office instructions to ensure USDA devices are updated in a timely manner with malicious code protection.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

[DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16, sets forth USDA's 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 shall be affected in accordance with applicable law and regulations.

Such disciplinary or adverse action shall be consistent with applicable law and regulations such as Office of Personnel Management regulations, Office of Management and Budget (OMB) regulations, and [Standards of Ethical Conduct for Federal Employees of the Executive Branch](#).

8. POLICY EXCEPTIONS

- a. All USDA agencies and staff offices are required to conform to this policy. In the event an agency or staff office cannot meet a specific policy requirement 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 the Departmental SOP by the ISC, [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1.
- b. Agencies and staff offices shall address all policy waiver request memorandums to the USDA CISO and submit the request to ISC.Outreach@wdc.usda.gov for review and decision. Unless otherwise specified, agencies and staff offices must review and renew approved policy waivers every fiscal year.

9. INQUIRIES

Direct all questions concerning this DR to Office of the Chief Information Officer (OCIO), Information Security Center (ISC), via email to the csc@ocio.usda.gov mailbox.

-END-

APPENDIX A

AUTHORITIES AND REFERENCES

CNSS, [CNSS Instruction \(CNSSI\) 4009](#), *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015

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

[Federal Records Act of 1950](#), 44 U.S.C. § 3101, 1950

National Archives and Records Administration (NARA), General Records Schedule ([GRS](#)) [3.1](#), *General Technology Management Records*, January 2017

NARA, [GRS 3.2](#), *Information Systems Security Records*, September 2016

NARA, [GRS 5.1](#), *Common Office Records*, July 2017

NARA, [GRS 5.2](#), *Transitory and Intermediary Records*, July 2017

NIST, [FIPS PUB 199](#), *Standards for Security Categorization of Federal Information and Information Systems*, February 2004

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

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

NIST, [SP 800-45](#) Version 2, *Guidelines on Electronic Mail Security*, February 2007

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 800-83](#) Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, July 2013

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

NIST, [SP 800-144](#), *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011

NIST, [SP 800-177](#), *Trustworthy Email*, September 2016

NIST, [SP 800-193](#), *Platform Firmware Resiliency Guidelines*, May 4, 2018

Office of Government Ethics, [*Standards of Ethical Conduct for Federal Employees of the Executive Branch*](#), 5 Code of Federal Regulations (CFR) § 2635, et seq., (2017)

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, December 2016

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

USDA, [*DM 3530-001*](#), *USDA Vulnerability Scan Procedures*, July 20, 2005

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

USDA, [*DM 3535-002*](#), *Chapter 7, Part 2 Patch Management and Systems Updates*, May 11, 2005

USDA, [*DR 1495-001*](#), *New Media Roles, Responsibilities and Authorities*, May 23, 2011

USDA, [*DR 3080-001*](#), *Records Management*, August 16, 2016

USDA, [*DR 3085-001*](#), *Vital Records Management Program*, August 19, 2011

USDA, [*DR 3099-001*](#), *Records Management Policy for Departing Employees, Contractors, Volunteers and Political Appointees*, July 2, 2012

USDA, [*DR 3300-001*](#), *Telecommunications & Internet Services and Use*, March 18, 2016

USDA, [*DR 3505-005*](#), *Cyber Security Incident Management Policy*, October 31, 2013

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

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

APPENDIX B

DEFINITIONS

Audit Record. An individual entry in an audit log related to an audited event. (Source: NIST SP 800-53 Revision 4)

Configuration Management. A collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems. (Source: NIST SP 800-128)

False Negative. An instance in which a security tool intended to detect a particular threat fails to do so. (Source: NIST SP 800-83 Revision 1)

False Positive. An instance in which a security tool incorrectly classifies benign content as malicious. (Source: NIST SP 800-83 Revision 1)

Flaw. Error of commission, omission, or oversight in an information system that may allow protection mechanisms to be bypassed. (Source: NIST Interagency Report (IR) 7298 Revision 2)

Indicator.

- a. Recognized action, specific, generalized, or theoretical, that an adversary might be expected to take in preparation for an attack. (Source: CNSS) 4009)
- b. A sign that an incident may have occurred or may be currently occurring. (Source: NIST IR 7298 Revision 2)

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. (Source: CNSSI 4009)

Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (Source: NIST SP 800-53 Revision 4)

Malicious Code. Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. (Source: NIST SP 800-53 Revision 4)

Malware. See Malicious Code.

Phishing. A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information. (Source: NIST IR 7298 Revision 2)

Records Management. The process for tagging information for records-keeping requirements as mandated in the *Federal Records Act* and the National Archival and Records Requirements. (Source: NIST IR 7298 Revision 2)

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 IR 7298 Revision 2)

Spam. The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (Source: NIST SP 800-53 Revision 4)

System Security Plan. Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. (Source: NIST SP 800-53 Revision 4)

Vulnerability. A weakness in a system, application, or network that is subject to exploitation or misuse. (Source: NIST IR 7298 Revision 2) See related term “flaw.”

APPENDIX C

ACRONYMS AND ABBREVIATIONS

CAPE	Compliance, Audit, Policy, and Enforcement
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COTS	Commercial Off-the-Shelf
DM	Departmental Manual
DR	Departmental Regulation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
GRS	General Records Schedule
IR	Interagency Report
ISC	Information Security Center
ISSPM	Information Systems Security Program Manager
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
PBX	Private Branch Exchange
POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SOP	Standard Operating Procedure
SOW	Statement of Work
SP	Special Publication
U.S.C.	United States Code
USDA	United States Department of Agriculture