

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

DEPARTMENTAL REGULATION	NUMBER: DR 3575-003
SUBJECT: Information Systems Log Retention Requirements	DATE: July 7, 2022
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: July 7, 2027

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

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) requirements for retaining, maintaining, and allowing access to information system logs. It guides all Mission Areas, agencies, and staff offices to implement Log Management Infrastructure (LMI), which consists of processes, personnel, and tools.
- b. To ensure USDA complies with Federal requirements to establish, implement, and enforce system activity logging and maintenance of logs that support the Department's management of information security risks to the USDA enterprise. This DR addresses and meets the requirements of:

(1) *Federal Information Security Modernization Act of 2014* (FISMA), [44 United States Code \(U.S.C.\) §§ 3551-3559](#);

- (2) Office of Management and Budget (OMB), Circular No. [A-123](#), *Management's Responsibility for Enterprise Risk Management and Internal Control*;
- (3) OMB, Circular No. [A-130](#), *Managing Information as a Strategic Resource*;
- (4) OMB, Memorandum [M-21-31](#), *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*;
- (5) National Institutes of Standards and Technology (NIST), Federal Information Processing Standards Publication [\(FIPS PUB\) 200](#), *Minimum Security Requirements for Federal Information and Information Systems*;
- (6) NIST, Special Publication [\(SP\) 800-53, Revision 5](#), *Security and Privacy Controls for Information Systems and Organizations*;
- (7) NIST, [SP 800-92](#), *Guide to Computer Security Log Management*; and
- (8) Record retention requirements in the National Archives and Records Administration (NARA) [General Records Schedules \(GRS\)](#).

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR is effective immediately when published and will remain in effect until superseded or expiration.
- b. All USDA Mission Areas, agencies, and staff offices must align their related Information Systems Log Retention policies with this DR within 6 months of the publication date.
- c. The term "USDA personnel" encompasses USDA employees, contractors, partners, interns, fellows, affiliates, and volunteers.

3. SCOPE

- a. This policy applies to all:
 - (1) USDA Mission Areas, agencies, staff offices, and personnel who implement or maintain information systems log retention procedures, plans, and functions;
 - (2) Federal information, in any medium or form, generated, collected, provided, transmitted, stored, maintained, processed, or accessed by, or on behalf of, USDA;
 - (3) Information systems, and cloud-based services used or operated by, for, or on behalf of USDA. These include interconnections between or among these

information systems or services;

(4) Facilities from which these systems or services operate, including:

(a) Facilities owned or operated by USDA; and

(b) Facilities owned or operated on behalf of USDA by a third party.

- b. This DR sets requirements for information system event logging, management of logs, and maintenance of LMI. It mandates implementing an LMI to identify and manage risks, consistent with the system categorization.
- c. Nothing in this policy alters the requirements for protecting national security systems or information. This includes those identified in policies, directives, instructions, and advisory memoranda issued by the Committee on National Security Systems ([CNSS](#)) or by the intelligence community.

4. BACKGROUND

- a. The planning activities for information system logging, maintenance of system logs, and management of LMI ensure logs are stored in sufficient detail for an appropriate or required period. Planning activities should properly scope, configure, and implement these capabilities.
- b. The USDA security information and event management (SIEM) system ingests logs from across the USDA enterprise to support investigations, response and recovery efforts.
- c. This DR specifies a model for evaluating the maturity level of system logging and management requirements defined in OMB, Memorandum M-21-31, which establishes requirements for Federal agencies to increase the sharing of log information, to accelerate incident response efforts and to enable more effective defense of Federal information systems and agencies.
- d. The LMI can filter, aggregate, normalize, and correlate logs to support event analysis. Efficient and effective log management balances resources with the required level of log data detail. The LMI also supports log confidentiality, integrity, and availability.

5. POLICY

- a. USDA Mission Areas, agencies, and staff offices will ensure practices and processes are in accordance with NIST SP 800-92 and OMB, Memorandum M-21-31.

- b. The Office of the Chief Information Officer (OCIO) Information Security Center (ISC) logging agent will be the primary logging capability on USDA assets. Auditable security events will be logged to support investigative actions, log review, analysis, and reporting in the USDA Enterprise Logging SIEM system. The technical logging details in OMB, Memorandum M-21-31, Appendix C, *Logging Requirements – Technical Details*, provide the common categories of auditable security events to be considered for mandatory logging and the log thereof retained for required periods of time.
- c. USDA Mission Areas, agencies, and staff offices may log additional information for moderate and high-impact systems, to achieve or maintain compliance with Federal log requirements.
- d. USDA Mission Areas, agencies, and staff offices will configure systems and tools to collect logs needed to support investigations, event reconstruction, metrics, and research.
- e. USDA Mission Areas, agencies, and staff offices will ensure that logs have the detail required to facilitate event reconstruction.
- f. USDA Mission Areas, agencies, and staff offices will encrypt the LMI and establish access controls in accordance with OMB, Memorandum M-21-31.
- g. USDA Mission Areas, agencies, and staff offices will ensure that log content for high-impact systems can be configured from a central location, are time-correlated, and implement non-repudiation measures.
- h. The LMI (tools, processes, and personnel) will support log retention requirements, including retention periods specified in OMB, Memorandum M-21-31, Appendix C. The USDA Enterprise Logging SIEM will:
 - (1) Allocate sufficient storage capacity to support OMB mandates;
 - (2) Maintain offline back-ups as required in OMB guidance; and
 - (3) Preserve logs in a manner that allows for centralized access.
- i. The USDA Enterprise Logging SIEM will be configured to:
 - (1) Overwrite the oldest logs during a log processing failure;
 - (2) Overwrite the oldest logs when storage capacity is exceeded for high-impact systems and cannot be shutdown based on mission needs or risk to the system; and
 - (3) Notify the Mission Area, agency, staff office, the USDA OCIO-ISC Security Operations Center (SOC), and other stakeholders of breaches, log failures, or when log storage reaches capacity.

- j. USDA Mission Areas, agencies, and staff offices will review, implement, and adhere to the time stamp schema defined in OMB, Memorandum M-21-31, Appendix A, *Implementation and Centralized Access Requirements*.
- k. USDA will apply the four-tier event logging (EL) maturity model defined in OMB, Memorandum M-21-31 to prioritize efforts, resources, and measure the level of compliance with logging and log management requirements. The four EL tiers that define compliance with requirements for implementation are:
 - (1) Tier EL0 has a rating of “Not Effective” indicating that logging requirements of highest criticality are either not met or are only partially met;
 - (2) Tier EL1 has a rating of “Basic” indicating that only logging requirements of highest criticality are met;
 - (3) Tier EL2 has a rating of “Intermediate” indicating that logging requirements of highest and intermediate criticality are met; and
 - (4) Tier EL3 has a rating of “Advanced” indicating that logging requirements at all criticality levels are met.
- l. USDA Mission Areas, agencies, and staff offices will ensure log management compliance, prioritizing high-impact systems and high value assets (HVA).
- m. Per [Executive Order 14028](#), *Improving America’s Cybersecurity*, and OMB, Memorandum M-21-31, the USDA SOC will share information with the Cybersecurity Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI).
- n. USDA Mission Areas, agencies, and staff offices will document and analyze lessons learned on their programs, control activities, procedures, and tasks. They will use this qualitative and quantitative data to assess effectiveness and to guide process improvement.

6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) will:
 - (1) Ensure the USDA logging and log management program is adequately funded; and
 - (2) Oversee the information technology (IT) resources that generate, transmit, and store the logs.

- b. The USDA Chief Information Security Officer (CISO) will:
 - (1) Coordinate with the CIO to ensure implementation of an LMI and compliance with Departmental logging and log management requirements;
 - (2) Coordinate with Mission Area Assistant CIOs to ensure information systems can perform required logging;
 - (3) Report to the CIO on the effectiveness of the logging and log management programs, including on violations of policy; and
 - (4) Review or approve enterprise risks via the Risk-Based Decision (RBD) process.
- c. Mission Area Assistant CIOs will ensure personnel with logging and log management responsibilities complete role-based training.
- d. Mission Area Assistant CISOs or Information Systems Security Managers (ISSM) will:
 - (1) Provide guidance for prioritizing the log management requirements and meeting the hardware and software requirements for information systems; and
 - (2) Ensure required event notifications are accurate and timely.
- e. The Director of the OCIO-ISC Cybersecurity Infrastructure Division (CSID) will:
 - (1) Implement an effective LMI to ensure central logging and secure retention of logs;
 - (2) Ensure Log Management Administrators coordinate with System Owners and Information Owners to:
 - (a) Maintain the LMI;
 - (b) Identify all systems required to forward logging data; and
 - (c) Configure their system logging functions to provide the required data; and
 - (3) Manage the validation of logging capabilities to ensure compliance.
- f. The Director of the OCIO-ISC Cyber Defense Operations Division (CDOD) will:
 - (1) Share information with CISA and the FBI; and
 - (2) Ensure the SOC notifies appropriate stakeholders of log failures or when log storage reaches capacity.

- g. System Owners will:
 - (1) Ensure information systems integrate with the LMI;
 - (2) Ensure the preservation of logs to support investigations, response and recovery efforts, and *Freedom of Information Act* ([FOIA](#)) requests; and
 - (3) Coordinate with the Information Owner when setting log retention requirements and time periods.
- h. Information Owners will:
 - (1) Inform the System Owner of information system log and log retention requirements; and
 - (2) Coordinate with Log Management Administrators and System Owners to ensure that all required logs are transferred to CDOD.
- i. Security Architects or Engineers will:
 - (1) Provide guidance for LMI solutions such as log collection, storage, and retrieval;
 - (2) Employ, configure, and test log capabilities; and
 - (3) Update log procedures, and log configurations as needed.
- j. Log Management Administrators, and System, Database, and Network Administrators will:
 - (1) Ensure the LMI aligns with OMB, Memorandum M-21-31, and NARA GRS retention requirements;
 - (2) Configure logging and log management capabilities to collect required data in accordance with authoritative references; and
 - (3) Manage the log failures, security, and storage processes.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

[DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16, sets forth USDA developed policies, procedures, and standards on employee responsibilities and conduct regarding the use of computers and telecommunication equipment. In addition, DR 4070-735-001, Section 21, *Disciplinary or Adverse Action*, states:

- a. Any violation of the responsibilities or standards contained in this DR may be cause for disciplinary or adverse action; and
- b. Any disciplinary or adverse action taken will be consistent with the applicable laws and regulations.

8. POLICY EXCEPTIONS

- a. All Mission Areas, agencies, and staff offices will conform to this policy. If any Mission Area, agency, or staff office cannot meet a specific policy requirement, they may request a policy exception via the RBD process. Note that an approved RBD is an acceptance of risk but does not constitute compliance with policy. Requests for a policy exception:
 - (1) Acknowledge the non-compliance with policy; and
 - (2) Document an acceptable plan to remediate the weakness, as indicated in the [POA&M-SOP-3540-003A](#), *Standard Operating Procedures (SOP) on Plan of Action & Milestones (POA&M) Management*.
- b. Submit policy exception requests to the Mission Area Authorizing Official (AO) in accordance with [RBD-SOP-3540-003B](#), *USDA Standard Operating Procedures on Risk-Based Decision Management*.

9. INQUIRIES

Send any questions or concerns about this DR to the OCIO, ISC via smd-pcb-policy@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

AO	Authorizing Official
CDOD	Cyber Defense Operations Division (OCIO-ISC component)
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISA	Cybersecurity Infrastructure Security Agency
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CSID	Cybersecurity Infrastructure Division (OCIO-ISC component)
DR	Departmental Regulation
EL	Event Logging
FBI	Federal Bureau of Investigation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FOIA	Freedom of Information Act
GRS	General Records Schedules
HVA	High Value Asset
ISC	Information Security Center (OCIO component)
ISSM	Information Systems Security Manager
IT	Information Technology
LMI	Log Management Infrastructure
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
POA&M	Plan of Action and Milestones
RBD	Risk-Based Decision
SIEM	System Information Event Management
SOC	Security Operations Center (OCIO-ISC component)
SOP	Standard Operating Procedure
SP	Special Publication
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: NIST, SP 800-53, Revision 5)

Log. A record of the events occurring within an organization's systems and networks. (Source: NIST, SP 800-92)

Log Management. The process for generating, transmitting, storing, analyzing, and disposing of log data. (Source: NIST, SP 800-92)

Log Management Infrastructure (LMI). The hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data. (Source: NIST, SP 800-92)

Non-Repudiation. Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message. (Source: NIST, SP 800-53, Revision 5)

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](#), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*)

Risk. The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals; resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (Source: [NIST, SP 800-30, Revision 1](#), *Guide for Conducting Risk Assessments*)

USDA Personnel. USDA employees, contractors, partners, interns, fellows, affiliates, and volunteers who work for, or on behalf of USDA. (Source: [DR 3530-006](#), *Scanning and Remediation of Configuration and Patch Vulnerabilities*)

APPENDIX C

AUTHORITIES AND REFERENCES

CNSS, [CNSS Instruction No. 4009](#), *Committee on National Security Systems (CNSS) Glossary*, March 2, 2022

CNSS, [Introducing the CNSS Library](#) website

[Executive Order 14028](#), *Improving the Nation's Cybersecurity*, May 12, 2021

Federal Information Security Modernization Act of 2014 (FISMA), [44 U.S.C. §§ 3551-3559](#), December 18, 2014, as amended

Freedom of Information Act (FOIA), [5 U.S.C. § 552](#), January 1, 1996 as amended by Public Law No. 104-231, 110 Stat. 3048, October 2, 1996, as amended

NARA, [General Records Schedules \(GRS\)](#) website

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

NIST, [SP 800-30, Revision 1](#), *Guide for Conducting Risk Assessments*, September 2012, as amended

NIST, [SP 800-37, Revision 2](#), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018, as amended

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

NIST, [SP 800-92](#), *Guide to Computer Security Log Management*, September 2006, as amended

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

OMB, Circular [No. A-123](#), *Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016

OMB, Circular [No. A-130](#), *Managing Information as a Strategic Resource*, July 28, 2016

OMB, Memorandum [M-21-31](#), *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021

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

USDA, [DR 3090-001](#), *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*, May 28, 2008, as amended

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

USDA, [DR 3450-002](#), *Freedom of Information Act Implementation Regulations*, February 7, 2003, as amended

USDA, [DR 3530-006](#), *Scanning and Remediation of Configuration and Patch Vulnerabilities*, June 5, 2019, as amended

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

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

USDA, OCIO, [POA&M-SOP-3540-003A](#), *Standard Operating Procedure (SOP) on Plan of Action & Milestones (POA&M) Management*, Version 1.3, September 2021

USDA, OCIO, [RBD-SOP-3540-003B](#), *USDA Standard Operating Procedure on Risk-Based Decision Management*, Version 1.6, September 2021