

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

DEPARTMENTAL REGULATION	NUMBER: DR 3445-001
SUBJECT: Media Protection	DATE: October 30, 2019
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: October 30, 2024

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Special Instructions/Cancellations	2
3. Background	2
4. Scope	3
5. Policy	4
6. Roles and Responsibilities	7
7. Penalties and Disciplinary Actions for Non-Compliance	10
8. Policy Exceptions	11
9. Inquiries	11
Appendix A - Authorities and References	A-1
Appendix B - Definitions	B-1
Appendix C - Acronyms and Abbreviations	C-1
Appendix D - Guidance for Transporting CUI	D-1

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy for protecting all forms of media that record and store either digital or non-digital information.
- b. It is USDA policy to comply with Federal requirements by establishing, implementing, and enforcing media protection policies and procedures to continually manage risks to USDA information, information systems, and services.
- 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](#); National Institute of Standards and Technology (NIST) [Federal Information Processing Standards \(FIPS\) Publication \(FIPS PUB\) 200](#), *Minimum Security Requirements for Federal Information and Information Systems*; and the NIST [Special Publication \(SP\) 800-53](#)

[Revision 4](#), *Security and Privacy Controls for Federal Information Systems and Organizations*.

- d. This policy provides the foundation for USDA Mission Areas, agencies, and staff offices to develop and implement media protection procedures that comply with Federal and Departmental requirements and align with USDA's media protection policy. Controlling access to digital and non-digital media, based on the information's sensitivity, is necessary to protect USDA personnel, missions, and business processes against malicious or unauthorized activities, and protect the confidentiality and integrity of USDA information.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy supersedes Section 3, items 8, 9, and 13 of [DM 3550-002](#), *Sensitive but Unclassified (SBU) Information Protection*.
- b. This policy is effective immediately and remains in effect until superseded or expired.
- c. All agencies will align their media protection procedures with this DR within 6 months of the publication date.
- d. The term "agencies" or "USDA agencies" will be considered to encompass all USDA Mission Areas, agencies, and staff offices, unless otherwise noted in this document.
- e. The term "USDA employee" means a Federal civil servant employed by, detailed, or assigned to USDA, including members of the Armed Forces.
- f. The term "USDA personnel" means USDA employees, contractors, affiliates, interns, fellows, and volunteers who work for, or on behalf of, USDA, and whose work is overseen by USDA employees.
- g. The term "client device" refers to a laptop or mobile device. This policy uses the term "client device" in place of the NIST term "telework client device;" and
- h. The term "Controlled Unclassified Information" (CUI) encompasses and replaces previous sensitive information labels (e.g., For Official Use Only (FOUO) and SBU), in accordance with [Executive Order \(E.O.\) 13556](#), *Controlled Unclassified Information*. The Office of Homeland Security (OHS) administers the Department's CUI Program.

3. BACKGROUND

Digital and non-digital media provide ways of recording and storing information and are represented by a variety of formats. Examples of digital media include magnetic media, such as disks or tapes; optical media, such as optical discs; and non-volatile storage media, such as flash drives, flash memory, solid state drives, and memory cards. Examples of non-digital media include paper documents and microfilm.

Many types of media (both digital and non-digital) are removable, portable, and may be easily misplaced, lost, or stolen. Protecting media reduces the risk of unauthorized information exposure (loss of confidentiality), information tampering (loss of integrity), or inability to access information when needed (loss of availability).

4. SCOPE

a. This policy applies to:

- (1) All USDA agencies and personnel who work for, or on behalf of, USDA;
- (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) and interconnections between or among information systems or services that are used or operated by USDA, USDA contractors, subcontractors, or other organizations on behalf of, or funded by, USDA; and
- (4) Facilities where 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. Media protection concepts contained in this document relate to other information security policies, procedures, and requirements including physical access controls and access control enforcement, rules of behavior, maintenance, contingency planning, incident management, information protection through cryptography and other means, and protecting CUI. DRs, Departmental Manuals (DM), agency-level policies and procedures, and standard operating procedures (SOP) related to these topics should be referred to as needed to enhance the utility of this DR.

c. This policy is closely related to other USDA policies, programs, and procedures, including:

- (1) DR 3xxx-xxx, *Bring Your Own Device (BYOD) Policy*;
- (2) [DR 3080-001](#), *Records Management*;
- (3) [DR 3440-001](#), *USDA Classified National Security and Controlled Unclassified Information Program*, (update forthcoming);
- (4) DR 35xx-xxx, *Privacy Policy and Compliance for Personally Identifiable Information (PII)*, (forthcoming);
- (5) [DR 3580-004](#), *Securing Remote Access to USDA Information Systems and Client Devices*;

- (6) [DR 3580-005](#), *Securing Client Devices for International Travel*; and
 - (7) [DR 3640-001](#), *Identity, Credential, and Access Management*.
- d. Nothing in this policy will alter the requirements for the protection of information associated with national security information or national security systems such as those identified in FISMA, policies and standards issued by the Committee on National Security Systems (CNSS), or intelligence community policies, directives, or instructions.

5. POLICY

- a. All USDA personnel will protect and control access to all types of media and information used by, or on behalf of, USDA.
- b. USDA agencies will create, update, and maintain processes and procedures implementing this policy and consistent with other USDA policies and procedures related to records management and CUI.
- c. Agencies will ensure that media are protected throughout the media's lifecycle and wherever located, whether in use, in storage, in transport, or during maintenance.
- d. Agencies will:
 - (1) Define appropriate use for [trusted and untrusted] removable media; and
 - (2) Implement automated mechanisms to prevent untrusted removable media from being used on devices owned or operated by, or on behalf of, USDA.
- e. Agencies will ensure that:
 - (1) All non-publicly available Federal information residing on removable digital media and client devices is encrypted when taken outside of USDA facilities;
 - (2) Digital and non-digital media that contain CUI are marked with the appropriate CUI category, handling instructions, and distribution caveats as indicated by the National Archives and Records Administration (NARA) [CUI Category Markings](#) list and the NARA handbook, [Marking Controlled Unclassified Information Version 1.1](#).
 - (3) Media containing PII are protected (e.g., media encryption, password protection, logging, and secure transport) in accordance with DR 35xx-xxx, *Privacy Policy and Compliance for Personally Identifiable Information (PII)*, (forthcoming);
 - (4) All media, including client devices, taken on international travel comply with the requirements in DR 3580-005;

- (5) All non-digital media containing non-publicly available Federal information are properly disposed of (e.g., shredded, burned) when no longer needed and consistent with NARA-approved records retention schedules;
 - (6) Digital media containing CUI are sanitized when the CUI is no longer needed, in accordance with USDA's records management policies and procedures; and
 - (7) Digital media are sanitized prior to being redeployed, undergoing maintenance, being decommissioned, retired, or disposed of to ensure unauthorized users do not obtain access to data stored by the previous user.
- f. Media protection procedures that comply with Federal and Departmental regulations will be developed, disseminated, implemented, and will, at a minimum:
- (1) Identify both digital and non-digital media to be protected;
 - (2) List the types of media or devices that are authorized to store USDA information;
 - (3) Define restrictions on uses of media or activities with media (e.g., transport or use on non-USDA systems) and the circumstances of the restrictions, as applicable, particularly when the media contain CUI; and
 - (4) Identify and describe roles and responsibilities for media protection activities.
- g. Procedures for media protection will also:
- (1) Specify who is authorized to access or use different types of media and under what circumstances (i.e., need-to-know), including, but not limited to, prohibitions or restrictions on the use of:
 - (a) Personally owned media and client devices, defined as BYOD in DR 3xxx-xxx;
 - (b) Removable media and client devices that connect to, or are a part of, sensitive USDA systems;
 - (c) Removable media and client devices containing USDA information that connect to, or are a part of, external information systems;
 - (d) Removable media, client devices, and other electronic devices (e.g., cameras, smart phones, and other portable media devices) with the capability to record or transmit in sensitive areas; and
 - (e) Removable media or portable storage devices that have no identifiable owner (e.g., media found unattended in public areas or free gifts from vendors).
 - (2) Specify physical and logical discretionary and non-discretionary access control methods for protecting access to different types of media;

- (3) Specify other technical safeguards, such as requirements to:
 - (a) Scan media for malicious code regularly or prior to use;
 - (b) Disable or remove the ability to insert, read, or write to media, or alternatively configure removeable media ports to “read only” and disable “read, write, execute” capabilities; and
 - (c) Encrypt non-publicly available information stored on the media, using FIPS approved encryption (i.e., NIST, [FIPS PUB 140-2](#), *Security Requirements for Cryptographic Modules*) and following guidelines in NIST [SP 800-111](#), *Guide to Storage Encryption Technologies for End User Devices*.
- (4) Specify acceptable methods and locations for securely storing the various types of media throughout the media’s lifecycle and restricting access to stored media containing non-publicly available Federal information, including but not limited to, media stored at:
 - (a) Facilities owned or operated by, or on behalf of, USDA; and
 - (b) Primary or alternate storage locations for contingency and disaster planning purposes.

Note: [DR 3571-001](#), *Information System Contingency Planning and Disaster Recovery Planning*, addresses the frequency and quality of digital information stored at alternate storage sites.

- (5) Specify acceptable methods for protecting and controlling different types of media during transport outside of controlled areas, commensurate with the information stored on the media, with requirements to include:
 - (a) Authorizing transport of media and the circumstances for doing so (i.e., business needs);
 - (b) Maintaining accountability for, and tracking of, the media through the transport process or a system to prevent or detect loss;
 - (c) Identifying acceptable protection methods, such as encryption, packaging, or locked containers to prevent unauthorized access, destruction, or tampering;
 - (d) Identifying cryptographic mechanisms to protect non-publicly available information stored on digital media during transport; and
 - (e) Indicating restrictions on transport methods (e.g., in personal vehicles) or destinations (e.g., outside the United States). Transportation of media will be in accordance with DR 35xx-xxx.

Note: Appendix D provides guidance for transporting CUI.

- (6) Specify requirements to mark digital and non-digital media that contain CUI with the information's CUI categories and associated distribution restrictions and handling caveats;
- (7) Reference DR 3080-001 or the NARA-approved records retention schedule to identify digital and non-digital media preservation requirements for information that is released for disposition (i.e., the transfer of permanent historical records or the migration or destruction of temporary records); and
- (8) Specify requirements to sanitize media prior to disposal, release out of organizational control, or release for reuse, to include:
 - (a) Employing sanitization mechanisms with the strength and integrity commensurate with the types of information residing on the media, (e.g., CUI category or non-publicly available information);
 - (b) Descriptions of the sanitization techniques and procedures to be employed, in accordance with the guidance in NIST [SP 800-88 Revision 1](#), *Guidelines for Media Sanitization*; and
 - (c) Specific requirements for media containing data from information systems categorized as high-impact, based on NIST, [FIPS PUB 199](#), *Standards for Security Categorization of Federal Information and Information Systems*, that include:
 - 1 Reviewing, approving, tracking, documenting, and verifying media sanitization and disposal actions;
 - 2 Testing sanitization equipment and reviewing procedures at least annually, to verify that the intended sanitization is being achieved; and
 - 3 Defining circumstances for nondestructive sanitization techniques for portable storage media before connecting them to an information system.

6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) will:
 - (1) Be the senior agency official responsible for media protection;
 - (2) Ensure the Department's media protection and sanitization goals are aligned with business objectives and risk management practices; and
 - (3) Collaborate with the OHS Director on matters involving CUI.
- b. The USDA Chief Privacy Officer (CPO) will:
 - (1) Provide oversight and guidance on PII issues; and

- (2) Coordinate with system owners and information stewards to ensure acceptable methods of protecting, controlling, and securing information, and ensure appropriate oversight before sanitizing information or media.
- c. The Departmental Records Officer will:
 - (1) Provide oversight and guidance on Federal and Departmental requirements for related records management and retention issues; and
 - (2) Coordinate with system owners and information stewards to ensure acceptable methods of protecting, controlling, and securing information, and ensure appropriate oversight before sanitizing information or media.
- d. The OHS Director will:
 - (1) Administer the Department's CUI Program (per E.O. 13556 and 32 CFR Part 2002);
 - (2) Provide oversight and guidance to agencies on Federal and Departmental CUI requirements; and
 - (3) Coordinate with system owners and information stewards to ensure acceptable methods of protecting, controlling, and securing information, and ensure appropriate oversight and coordination before sanitizing information or media, particularly when involving CUI.
- e. The USDA Chief Information Security Officer (CISO) will:
 - (1) Ensure that the Department's information security program and plans adequately address media protection and are updated accordingly as Federal requirements for media protection change; and
 - (2) Provide compliance oversight and guidance to agencies on Federal and Departmental requirements for media protection.
- f. Mission Area Assistant CIOs will:
 - (1) Ensure that procedures for media protection are developed, implemented, and updated as needed and that they comply with Federal and Departmental requirements; and
 - (2) Ensure that all personnel are aware of media protection requirements.
- g. Mission Area Assistant CISOs and Information Systems Security Program Managers (ISSPM) will:
 - (1) Coordinate with the USDA CPO, Departmental Records Officer, OHS Director, and information stewards to ensure acceptable methods of protecting, controlling,

and securing information are applied and appropriate procedures and safeguards are employed before sanitizing information or media;

- (2) Develop, disseminate, and update agency procedures for media protection;
- (3) Ensure that rules of behavior include media protection requirements; and
- (4) Provide oversight and guidance on compliance with all media protection requirements.

h. Information Stewards will:

- (1) Coordinate with system owners to assign roles and define responsibilities for marking, protecting, and securely storing information or media;
- (2) Review agency media protection procedures to ensure they address all requirements, provide guidance to address any gaps in the procedures, and ensure agency personnel implement and follow the procedures;
- (3) Ensure media protection procedures address requirements for protecting any media which:
 - (a) Contain CUI or PII;
 - (b) Are transported outside of USDA-controlled facilities; or
 - (c) Are being taken on, or returning from, international travel.
- (4) Coordinate with system, database, and network administrators to ensure that media are properly sanitized prior to disposal, release out of organizational control, or release for reuse.

i. System Owners will:

- (1) Document media protection lifecycle requirements as part of their system security plans (SSP), including, but not limited to:
 - (a) Appropriate levels of protection based on the types of information (e.g., CUI or other non-publicly available information) stored on various types of media;
 - (b) Backup media and transport to alternate storage; and
 - (c) Roles and responsibilities, including but not limited to, marking media and media sanitization.
- (2) Ensure that media for their systems are properly marked, stored, and transported; and

- (3) Verify through the Office of the General Council that the media and information are not subject to electronic discovery litigation or other legal requirements or restrictions prior to sanitizing, disposing of, or destroying the media.
- j. System, Database, and Network Administrators will:
- (1) Complete the annual Information Security Awareness Training course, which includes many aspects of media protection, in accordance with [DR 3545-001](#), *Information Security Awareness and Training Policy*, and any necessary training on CUI marking and protection requirements at the NARA [CUI Training Tools](#) website;
 - (2) Comply with all Federal and Departmental media protection requirements and rules of behavior included in the Information Security Awareness Training course;
 - (3) Properly mark all system media, as applicable; and
 - (4) Ensure that media are properly sanitized prior to disposal, release out of organizational control, or release for reuse.
- k. All USDA Personnel will:
- (1) Complete the annual Information Security Awareness Training course, which includes many aspects of media protection, in accordance with DR 3545-001;
 - (2) Comply with all Federal and Departmental media protection requirements and rules of behavior included in the Information Security Awareness Training course;
 - (3) Follow documented procedures for using, storing, and transporting digital and non-digital media;
 - (4) Promptly report lost or stolen digital or non-digital media, in accordance with incident reporting policy and procedures; and
 - (5) Report misuse or abuse of media to appropriate authorities.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

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

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

Such disciplinary or adverse action will be consistent with applicable law and regulations, such as Office of Personnel Management or Office of Management and Budget (OMB) regulations and the *Standards of Ethical Conduct for Federal Employees of the Executive Branch*. [5 Code of Federal Regulations \(CFR\) Part 2635](#).

8. POLICY EXCEPTIONS

- a. All USDA agencies are required to conform to this policy. If an agency cannot meet a 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; and
 - (2) Must be documented as indicated in [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1.
- b. Policy waiver request memoranda will be addressed to the USDA CISO and submitted to ISC.Outreach@usda.gov for review and decision. Unless otherwise specified, approved policy waivers must be review and renewed every fiscal year.

9. INQUIRIES

Address inquiries concerning this DR to the Office of the Chief Information Officer, Information Security Center 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

Controlled Unclassified Information (CUI), [32 Code of Federal Regulations \(CFR\) Part 2002](#), (2017)

[E.O. 13556](#), *Controlled Unclassified Information*, November 9, 2010

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

Fraud and related activity in connection with identification documents, authentication features, and information, U.S.C. [18 U.S.C. § 1028\(d\)\(7\)](#), (2017)

NARA, [CUI: Additional Tools](#)

NARA, [CUI Categories](#)

NARA, [CUI Category Markings](#)

NARA, [CUI Training Tools](#)

NARA Handbook, [Marking Controlled Unclassified Information, Version 1.1](#), December 6, 2016

NIST, Computer Security Resource Center, [Glossary](#)

NIST, [FIPS PUB 140-2](#), *Security Requirements for Cryptographic Modules*, December 3, 2002

NIST, [FIPS PUB 199](#), *Standards for Security Categorization of Federal Information and Information Systems*, February 1, 2004

NIST, [FIPS PUB 200](#), *Minimum Security Requirements for Federal Information and Information Systems*, March 1, 2006

NIST, [SP 800-46 Revision 2](#), *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, July 2016

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 800-88 Revision 1](#), *Guidelines for Media Sanitization*, December 17, 2014

NIST, [SP 800-111](#), *Guide to Storage Encryption Technologies for End User Devices*, November 15, 2007

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

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

USDA, [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, revision 1.1, November 2015

USDA, [DM 3440-001](#), *USDA Classified National Security Information Program Manual*, June 9, 2016

USDA, [DM 3550-002](#), *Sensitive but Unclassified (SBU) Information Protection*, February 17, 2005

USDA, DR 3xxx-xxx, *Bring Your Own Device (BYOD) Policy*, forthcoming

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

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

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

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

USDA, [DR 3410-001](#), *Information Collection Activities – Collection of Information from the Public*, May 6, 2009

USDA, [DR 3440-001](#), *USDA Classified National Security and Controlled Unclassified Information Program*, June 9, 2016 (update forthcoming)

USDA, DR 35xx-xxx, *Privacy Policy and Compliance for Personally Identifiable Information (PII)*, (forthcoming)

USDA, [DR 3545-001](#), *Information Security Awareness and Training Policy*, November 22, 2013

USDA, [DR 3571-001](#), *Information System Contingency Planning and Disaster Recovery Planning*, June 1, 2016

USDA, [DR 3580-004](#), *Securing Remote Access to USDA Information Systems and Client Devices*, November 30, 2018

USDA, [DR 3580-005](#), *Securing Client Devices for International Travel*, November 30, 2018

USDA, [DR 3640-001](#), *Identity, Credential, and Access Management*, December 9, 2011

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

USDA, [DR 4080-811-002](#), *Telework Program*, January 4, 2018

APPENDIX B

DEFINITIONS

Bring Your Own Device (BYOD). A non-organization-controlled telework client device. These client devices are controlled by the teleworker, who is fully responsible for securing them and maintaining their security. (Source: NIST, SP 800-46 Revision 2). Also refer to USDA, DR 3xxx-xxx, *Bring Your Own Device (BYOD) Policy* (forthcoming).

Clear. A method of sanitization by applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). (Source: NIST, SP 800-88 Revision 1)

Controlled Unclassified Information (CUI). Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and governmentwide policies but is not classified under [E.O. 13526](#), *Classified National Security Information*, or the *Atomic Energy Act*, [42 U.S.C. § 2011](#), as amended. (Source: E.O. 13556, *Controlled Unclassified Information*)

Cryptographic Erase. A method of Sanitization in which the Media Encryption Key (MEK) for the encrypted Target Data (or the Key Encryption Key – KEK) is sanitized, making recovery of the decrypted Target Data infeasible. (Source: NIST, SP 800-88 Revision 1)

Cryptography. Art or science concerning the principles, means, methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form. (Source: CNSS, CNSSI-4009)

Destroy. A method of sanitization that renders target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the media for storage of data. (Source: NIST, SP 800-88 Revision 1)

Encryption. The process of changing plaintext into ciphertext. (Source: NIST, Computer Security Resource Center, *Glossary*)

Federal Information. Information created, collected, processed, maintained, disseminated, or disposed of by, or for, the Federal Government in any medium or forum. (Source: OMB, Circular A-130)

Federal Information System. An information system used or operated by an executive Agency, by a contractor of an executive Agency, or by another organization on behalf of an executive Agency. (Source: NIST, SP 800-53 Revision 4)

Information Steward. Individual or group that helps to ensure the careful and responsible management of Federal information belonging to the Nation as a whole, regardless of the

entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to Federal information to elements of the Federal Government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance. (Source: NIST, Computer Security Resource Center, *Glossary*)

Media. Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. See also singular “Medium.” (Source: NIST, SP 800-53 Revision 4)

Media Sanitization. A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. (Source: NIST, SP 800-88 Revision 1)

Medium. Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs. (Source: NIST, SP 800-88 Revision 1)

Mobile Device. A small mobile computer such as a smartphone or tablet. (Source: NIST, SP 800-46 Revision 2)

Personally Identifiable Information (PII). Any information about an individual maintained by an Agency, including (1) any information that can be used to distinguish or trace an individual’s identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Source: NIST, Computer Security Resource Center, *Glossary*)

Purge. A method of sanitization by applying physical or logical techniques that renders target data recovery infeasible using state-of-the-art laboratory techniques. (Source: NIST, SP 800-53 Revision 4)

Removable Media. Portable data storage medium that can be added to or removed from a computing device or network. (Source: CNSS, CNSSI-4009)

Sanitization. Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs. (Source: NIST, SP 800-53 Revision 4)

Sanitize. A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media. (Source: NIST, SP 800-88 Revision 1)

Storage. Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered, and from which data may be retrieved. (Source: NIST, SP 800-88 Revision 1)

Target Data. The information subject to a given process, typically including most or all information on a piece of storage media. (Source: NIST, SP 800-88 Revision 1)

APPENDIX C

ACRONYMS AND ABBREVIATIONS

BYOD	Bring Your Own Device
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
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
DM	Departmental Manual
DR	Departmental Regulation
E.O.	Executive Order
FIPS	Federal Information Processing Standards
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FOUO	For Official Use Only
ISSPM	Information Systems Security Program Manager
KEK	Key Encryption Key
LSI	Large-Scale Integration
MEK	Media Encryption Key
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
OHS	Office of Homeland Security
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SBU	Sensitive but Unclassified
SOP	Standard Operating Procedure
SP	Special Publication
SSP	System Security Plan
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX D

GUIDANCE FOR TRANSPORTING CUI

USDA processes all types of CUI, and it is essential that this information be properly handled and protected. The following steps are necessary when physically transporting digital (e.g., flash drive, memory card, optical disk) or non-digital media (e.g., paper, microfilm).

- a. Obtain permission from your supervisor or manager to transport the information using an approved transportation method and ensure the recipient of the information is authorized to receive it.
- b. Encrypt digital media containing CUI using a NIST-approved encryption method.
- c. When the digital media is encrypted, securely transmit the decryption key separately.
- d. Mark physical and digital documents containing CUI using guidance provided by NARA's *Banner Format and Marking Notes*, which can be found using the [CUI Category Markings](#) website and NARA Handbook: [Marking Controlled Unclassified Information, Version 1.1](#).
- e. Double wrap digital and non-digital portable media as indicated below, using an opaque package or container that is sealed sufficiently to prevent inadvertent opening and will show signs of tampering:
 - (1) Mark documents properly and include the name and address of the recipient;
 - (2) Place the media in an opaque inner envelope;
 - (3) Cover all envelope seams with tamper-resistant tape (e.g., duct, packing, or acrylic tape);
 - (4) Affix classification markings to the inner envelope. Markings must be clear on the inner envelope. Address the inner envelope to the recipient by name;
 - (5) Insert the inner envelope into another opaque envelope and seal it. This becomes the outer wrapping;
 - (6) Do not put CUI markings on the outer wrapping; and
 - (7) Address the outer wrapping. The recipient's name on the outer wrapping is optional if hand carrying the package but is required when sent via authorized delivery service (per 32 CFR § 2002.14: U.S. Postal Service or any commercial delivery service).
- f. Transport Options:

- (1) U.S. Postal Service or commercial delivery service that provides the capability to track pickup, receipt, transfer, and deliver;
- (2) Interoffice mail when double-wrapped to afford sufficient protection against inadvertent or unauthorized access; or
- (3) Hand carried by USDA personnel:
 - (a) Maintain control of the package;
 - (b) Keep the package within direct sight, or in a container (e.g., backpack, purse or briefcase, carry-on luggage) that is within direct sight;
 - (c) Secure the package when leaving it unattended, such as by:
 - 1 Placing the package in a hotel room safe;
 - 2 Placing the package in a locked office or inside a drawer or file cabinet within a Federal building or facility;
 - 3 Storing the package in a desk drawer, cabinet, or an office space in the person's home; or
 - 4 Placing the package inside the locked trunk of a motor vehicle.
 - (d) Do not place the package in checked baggage; and
- (4) Only ship CUI abroad using the State Department diplomatic courier program when available and with the approval of the Agency Authorizing Official. Double wrap the portable media prior to transferring control to the State Department.

For additional information about the USDA CUI program or if you have questions or concerns related to CUI, please contact your agency point of contact for guidance and assistance. If you suspect or know that a CUI incident has occurred, please contact either the [USDA CUI Program Manager](#) or the ASOD Security Operations Center 24/7 help line at cyber.incidents@asoc.usda.gov or 1-877-744-2968.