

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

DEPARTMENTAL REGULATION	NUMBER: DR 3580-005
SUBJECT: Securing Client Devices for International Travel	DATE: November 30, 2018
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: November 30, 2023

<u>Section</u>	<u>Page</u>
1. Purpose	1
2. Scope	2
3. Special Instructions/Cancellations	3
4. Background	4
5. Policy	5
6. Roles and Responsibilities	9
7. Penalties and Disciplinary Actions for Non-Compliance	13
8. Policy Exceptions	13
9. Inquiries	14
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 policy for secure remote access to United States Department of Agriculture (USDA) information and information systems prior to, during, and upon return from foreign locations.
- b. It is USDA policy to comply with Federal requirements to establish, implement, and enforce a policy on:
 - (1) USDA information systems that facilitate remote access from international locations; and
 - (2) The use of devices and removable media when used to remotely access USDA information systems from international locations.
- c. This policy complies with the requirements of:

- (1) The *Federal Information Security Modernization Act of 2014* ([FISMA](#));
 - (2) Federal Information Processing Standards Publication ([FIPS PUB](#)) 200, *Minimum Security Requirements for Federal Information and Information Systems*;
 - (3) National Institute of Standards and Technology (NIST), [Special Publication \(SP\) 800-53 Revision 4](#), *Security and Privacy Controls for Federal Information Systems and Organizations*;
 - (4) NIST, [SP 800-46 Revision 2](#), *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*;
 - (5) NIST, [SP 800-114 Revision 1](#), *User's Guide to Telework and Bring Your Own Device (BYOD) Security*;
 - (6) NIST, [SP 800-124 Revision 1](#), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*;
 - (7) Office of Management and Budget (OMB), Memoranda [M-11-27](#), *Implementing the Telework Enhancement Act of 2010: Security Guidelines*;
 - (8) OMB, [M-17-12](#), *Preparing for and Responding to a Breach of Personally Identifiable Information*; and
 - (9) [Telework Enhancement Act of 2010](#).
- d. This policy serves as the foundation for agencies and staff offices to develop and implement foreign remote access policies and procedures that comply with Federal and Departmental requirements.

2. SCOPE

- a. This policy applies to:
- (1) All USDA Mission Areas, agencies, staff offices, employees, appointees, contractors, and others who work for, or on behalf of, USDA and use, or are responsible for, maintaining USDA information systems remotely accessed by devices or use removable media from international locations; and
 - (2) All Federal information, in any medium or form, generated, collected, provided, transmitted, stored, maintained, or accessed by, or on behalf of, USDA and all information systems or services (including cloud-based services) used or operated by USDA, USDA contractors, or other organizations on behalf of, or funded by, USDA.
- b. This directive builds on other information security policies that cover application and client device security requirements used domestically. However, this DR is written with

an emphasis on specifying requirements for ensuring the security of USDA information systems when individuals remotely access them from foreign locations. Related policies include:

- (1) [DR 3505-003](#), *Access Control for Information and Information Systems*, forthcoming;
 - (2) [DR 3580-004](#), *Securing Remote Access to USDA Information Systems and Client Devices*, November 30, 2018; and
 - (3) DR 35xx-xxx, *Bring Your Own Device*, forthcoming.
- c. Users should comply with [DR 5400-007](#), *Text Messaging While Driving*, which provides safety guidance about the use of Government furnished equipment while driving.
 - d. Nothing in this policy will alter the requirements of [DR 4080-811-002](#), *Telework Program*, that defines approved worksites for USDA, when those worksites may be used, and the conditions in which they may be used.
 - e. Nothing in this policy will alter the requirements for the protection of information associated with national security systems such as those identified in FISMA, policies, directives, instructions, and standards issued by the Committee on National Security Systems (CNSS), or the intelligence community.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy is effective immediately and remains in effect until superseded.
- b. All agencies and staff offices will align their international remote access policies and procedures with this policy within 6 months of the publication date.
- c. This DR uses the term “remote client device” in place of NIST’s “telework client device.” The two categories of client devices used in this policy and defined by NIST are:
 - (1) Personal computers (PC) (e.g., desktops and laptops); and
 - (2) Mobile devices (e.g., smartphones, tablets).

Note: The term “remote client device” in this DR encompasses any device in the two categories of devices used to remotely access USDA information systems.

- d. USDA desktop computers within USDA facilities that access USDA information systems do not need the same security requirements as remote client devices that access USDA information systems remotely. Section 5a addresses USDA desktop requirements when they remotely access USDA facilities.

- e. The term “controlled unclassified information” (CUI) replaces and encompasses all previous terms and labels for sensitive information such as for official use only (FOUO), sensitive but unclassified (SBU), Sensitive Security Information (SSI), and personally identifiable information (PII). The categories of CUI can be found in the National Archives and Records Administration (NARA) CUI [Registry – Categories and Subcategories](#).
- f. The term “burner” refers to a client device that cannot be sanitized to meet NIST [SP 800-88 Revision 1](#), *Guidelines for Media Sanitization* requirements and is to be used once; the primary use is during foreign travel to a country of high risk .
- g. The term “Government furnished” followed by “equipment,” “device,” or their plural forms will be used to describe the category of devices whose security posture is managed by USDA. The term is used in place of “Organization-Controlled Device,” which NIST uses and is defined in Appendix B.
- h. The terms “international travel” and “foreign travel” apply to trips, as well as permanent duty assignments in any country, territory, or commonwealth outside of the United States and its territories.
- i. The term “wireless” refers to client devices, (e.g., laptops, mobile devices) and networking devices (e.g., access points) exchanging data through radio communication within a limited geographic area, such as an office building.
- j. Wi-Fi is a trademark of the Wi-Fi Alliance.

4. BACKGROUND

The USDA remote access infrastructure affords personnel convenient and efficient methods to use USDA resources from external locations. However, remote client devices used to perform work from foreign locations introduce additional risks to USDA information and information systems; therefore, these devices have additional security requirements than those operating within USDA controlled areas and those operating from remote locations within the United States and its territories.

System owners that permit access to information systems from foreign locations must safeguard USDA information systems from threats arising from the lack of physical security controls, the use of insecure networks, and potentially compromised client devices used by personnel on foreign travel. Personnel using remote client devices are responsible for protecting them by knowing when, where, and how the devices are permitted to be used. Foreign governments are very skilled at collecting information even from devices that are turned off. Devices and sensitive information taken to foreign countries are susceptible to infection and compromise. Infected devices may not be discovered upon return and, if reconnected to USDA networks, may compromise the security of additional information. For these reasons, the Department strongly discourages personnel from taking devices to foreign countries.

Personnel should be mindful of restrictions on electronic equipment that may be brought aboard aircraft and that the restrictions may change without notice. The Department of Homeland Security and, potentially, the Department of State websites may have updated information about restrictions on electronic equipment. Employees can obtain security and threat briefings prior to traveling by following the guidance below and, when on travel with an official U.S. passport, by scheduling a security and threat briefing at a U.S. Embassy or Consulate.

5. POLICY

- a. Government furnished desktop computers, when used remotely from international locations to access or store USDA information, will have the same information storage, configuration, operational, and sanitization requirements as laptops in this DR.
- b. International travel locations identified as “a country of high risk” are based on:
 - (1) The ISSPM, based on information about the traveler’s destination in the Department of State [Travel Advisories](#) or [Travel to High-Risk Areas](#) web pages;
 - (2) Information provided by the ASOD Threat Intelligence team; and
 - (3) Information provided by Office of Homeland Security (OHS) Personnel and Document Security Division (PDSO).
- c. Agencies and staff offices whose personnel travel to a country of high risk will have a process with OHS PDSO to obtain a high-risk travel briefing.
 - (1) Personnel with security clearances will request a high-risk travel briefing by sending an email to pdsd@dm.usda.gov; and
 - (2) All other personnel will use the OHS [Foreign Travel Information](#) web page.

Additional responsibilities and duties described in [Departmental Manual \(DM\) 3440-001](#), *USDA Classified National Security Information Program Manual*, apply to Information Security Coordinators (ISC) and to personnel with national security clearances traveling internationally.

- d. Agencies and staff offices will ensure their personnel have international travel security and threat awareness information that reflects current and relevant changes to the threat environment for the traveler’s foreign destinations and includes but is not limited to:
 - (1) Unclassified threat information obtained from the Department of State’s *Travel Advisories* and *Travel to High-Risk Areas* web pages;
 - (2) Cybersecurity and physical threats in the foreign countries;

- (3) The cybersecurity controls required for remote client devices that will be used during international travel;
 - (4) Requirements for physical protection of remote client devices and removable media contained in this policy;
 - (5) Requirements for protection of CUI, including restrictions on printing;
 - (6) Prohibited use of public wireless networks in foreign countries; and
 - (7) Restricted use of Bluetooth in foreign countries.
- e. Agencies and staff offices will provide a fully patched, securely configured USDA wireless router to personnel whose international permanent duty station is outside of a U.S. Embassy, consulate, or other U.S. Federal building. The routers will include the following settings:
 - (1) Enable Wi-Fi Protected Access 2, often displayed as “WPA2/Enterprise;”
 - (2) Disable Wi-Fi Protected Setup; and
 - (3) Enable strong shared key.
 - f. Agencies and staff offices will use diplomatic pouches to deliver Government furnished devices and removable media to personnel whose permanent duty station is in a foreign location or when countries prohibit travelers from hand carrying electronic devices while traveling.
 - g. Government furnished remote client devices and removable media used domestically will only be taken on international travel when:
 - (1) Supporting USDA business functions;
 - (2) The USDA employee has obtained approval from their supervisor; or
 - (3) For contract support staff, the contractor has obtained approval from the Contracting Officer’s Representative (COR); and
 - (4) When a waiver has been submitted and approved.
 - h. An approved waiver will be required to take government furnished remote client devices and removable media to a country of high risk.
 - i. Personnel whose BYOD or third-party-controlled mobile device is provisioned in USDA’s BYOD program will follow the requirements in DR 35xx-xxx, *Bring Your Own Device*, prior to and upon return from international travel.
 - j. Agencies and staff offices that permit client devices to be taken outside the United States will:

- (1) Maintain an inventory of loaner and burner client devices and basic cell phones (non-smartphones with only voice and text capability) to be issued and used during international travel, or have an alternate process to harden Government furnished remote client devices used domestically and authorized for use on foreign travel;
- (2) Assess the risk of bringing such devices and removable media into the foreign country, including the risks of theft, confiscation, breach of data confidentiality and integrity, communications intercept, the insertion of malware into the devices, and unsuccessful sanitization;
- (3) Have procedures to:
 - (a) Assess the threat capabilities in the traveler's destinations using threat intelligence from the ASOD's threat intelligence team and, when necessary, their agency or staff office ISC or OHS PDSD;

Contact ASOD, 30 days in advance of travel via email to the cyberthreat@asoc.usda.gov mailbox to determine whether a country to be visited is a country of high risk.
 - (b) Ensure the devices are appropriately configured based on the threat intelligence about the foreign destination prior to being taken on international travel; and
 - (c) Arrange shipment of Government furnished devices and removable media via diplomatic pouch with U.S. Embassies or U.S. consulates.
- (4) Configure such devices to meet domestic security controls plus the following international travel requirements:
 - (a) Ensure basic cell phones only have voice and text capabilities;
 - (b) Disable Bluetooth and wireless networking services, and instruct the user on how to enable these services when needed and disable them again when not needed;
 - (c) Instruct users to conduct remote client device data communications to USDA information systems over cellular networks using a Virtual Private Network (VPN);
 - (d) Enroll mobile devices into a Mobile Device Management (MDM) solution, and add the provisioning profile that establishes an encrypted container;
 - (e) Equip laptops without an internal storage disk, but with an external hard drive or bootable disk image that the user can remove and store separately from the PC; and
 - (f) When permitted by the Authorizing Official (AO), provision such devices with email and file space accessible only through an encrypted container.

- (5) Identify the remote client device and removable media returning from a country not of high risk and:
 - (a) Quarantine them from connecting to information systems and services until the device and media have been assessed for and deemed free of malware, unauthorized executables, and other changes;
 - (b) Obtain approval from the Mission Area Assistant Chief Information Security Officer (CISO) or Information Systems Security Program Manager (ISSPM) to authorize moving the information from a client device or media that has malware, unauthorized executable code, or other unauthorized changes to USDA information system;
 - (c) Have techniques to securely move information from the client device or media to USDA information systems; and
 - (d) Sanitize the client device or media as specified in SP 800-88 Revision 1 if it has malware, unauthorized executable code, or other unauthorized changes.
- k. Government furnished remote client devices, removable media, and cell phones returning from a country of high risk will:
 - (1) Not be connected to USDA networks and information systems;
 - (2) At the agency or staff office discretion, require a forensic image made by either:
 - (a) The agency or staff office security operations team if one exists; or
 - (b) The USDA forensics team with Agriculture Security Operations Division (ASOD) Computer Security Incident Response Team (CSIRT) by sending an email message to cyber.incidents@asoc.usda.gov.
 - (3) Be sanitized in accordance with guidance in SP 800-88 Revision 1.
- l. Personnel on international travel will:
 - (1) Obtain foreign travel security and threat awareness information from the Department of State website, and when necessary, from OHS PDSD when traveling to a country of high risk prior to departure;
 - (2) Take the minimum amount of CUI and authorized applications needed to conduct USDA business on a loaner or burner remote client device during international travel;
 - (3) Only use removable media purchased in the 50 states or U.S. territories;
 - (4) Not connect removable media used with Government furnished client devices, including loaners or burners, to non-Government devices;

- (5) Not connect Government furnished remote client devices to non-Government equipment, including removable media, in accordance with [DR 3520-002](#), *Configuration Management*;
 - (6) Keep remote client devices and removable media within sight at all times or stored in a locked office or file cabinet at a U.S. Government owned and protected building such as a U.S. military base, U.S. Embassy, or U.S. consulate; and
 - (7) Not store remote client devices in checked baggage.
- m. Transmission, storage, and printing of CUI while on international travel is prohibited unless the actions take place in a pre-approved secure location such as:
 - (1) In a non-public room using a Government furnished local, non-networked printer;
 - (2) At a USDA in-country office location; or
 - (3) At other in-country U.S. Government offices such as the U.S. Embassy, consulate, or approved telecommunications services locations.
 - n. To minimize the opportunity for unauthorized foreign access mobile devices, and cell phones will:
 - (1) Be powered off when not in use. If possible, the battery and the subscriber identity module (SIM) card will be removed and stored separately from the device; or
 - (2) Be kept in airplane mode when in use and not transmitting or receiving information.
 - o. Personal Identity Verification (PIV) cards, Government furnished remote client devices, or cell phones lost, stolen, or confiscated while on international travel will be reported to the Department, agency, or staff office incident response team and the local U.S. Embassy or consulate immediately upon discovery. The ASOD CSIRT 24-hour contact information is 1-866-905-6890 or 816-823-1068, or the Cyber mailbox (cyber.incidents@asoc.usda.gov).
 - p. Personnel will also report the loss or theft of their PIV card to their PIV credential sponsor.

6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) will:
 - (1) Provide ongoing funding and support for the Departmental information security program and resources to support international travel; and
 - (2) Ensure policies and procedures governing foreign travel security are developed, disseminated, and implemented.

- b. The USDA CISO will:
 - (1) Oversee and ensure compliance with Federal and Departmental policies, procedures, and guidance on international travel issued to agencies and staff offices;
 - (2) Ensure the Department's business continuity plans and continuity of operation plans take into consideration risks posed by international travel and risks to USDA facilities located in foreign countries and territories;
 - (3) Provide guidance to USDA agencies and staff offices to ensure implementation of and compliance with Departmental requirements for information security while on international travel;
 - (4) Adjudicate requests for waivers from device sanitizing requirements; and
 - (5) Ensure that user training includes requirements and techniques to protect and properly secure remote client devices while on international travel.
- c. The Director of ASOD will:
 - (1) Coordinate the necessary actions to remotely track, purge, and disable lost or stolen remote client devices; and
 - (2) Coordinate with agencies or staff offices, or conduct forensic analysis on remote client devices returning from foreign countries.
- d. The Director of OHS will:
 - (1) Assess all requests for High-Risk Travel Briefings, and provide information only to personnel with a need-to-know and who have a national security clearance; and
 - (2) Have a process to ensure each agency or staff office can obtain high-risk travel briefings and personal safety, security, and country threat information from OHS PDSD.
- e. Agency and Staff Office AOs will:
 - (1) Be responsible for risk-based decisions regarding use of USDA-issued remote client devices used on and returning from international travel; and
 - (2) Adjudicate and approve, only for compelling mission and operational needs, requests for waivers from requirements that restrict:
 - (a) Whether remote client devices will be taken on international travel;
 - (b) Whether remote client devices taken on international travel will have email and file space access to USDA information systems; and

- (c) Whether information may be removed from remote client devices returning from international travel that have malware or unauthorized configuration changes.
- f. Mission Area Assistant CIOs will:
 - (1) Ensure CISOs and ISSPMs have adequate resources including funding, personnel, and training to implement and support the remote access infrastructure and remote client device security for international travel requirements; and
 - (2) Ensure remote access architectures protect the agency or staff office computing environments and information resources from malicious activity.
- g. Mission Area Assistant CISOs and ISSPMs will:
 - (1) Ensure a quarantine environment is available for remote client devices and removable media returning from international travel to ensure they have been scanned for malware, unauthorized executable code, and other unauthorized changes prior to connecting to information systems;
 - (2) Determine whether remote client devices or media returning from a country of high risk requires a forensic image before they are destroyed;
 - (3) Determine whether to approve or deny requests:
 - (a) To store CUI on a remote client device prior to it being taken to a foreign location; or
 - (b) To access or use CUI in a foreign location.
 - (4) Ensure processes and procedures are developed that:
 - (a) Ensure personnel traveling internationally receive information on the secure use and protection of remote client devices and removable media specific to the countries to be visited;
 - (b) Require personnel to comply with access control and training requirements prior to taking Government furnished remote client devices on foreign travel;
 - (c) Implement secure configuration baselines for remote client devices taken on international travel based on threat intelligence and risk assessments;
 - (d) Ensure approval is obtained prior to CUI being taken to, or used in, a foreign location;
 - (e) Ensure Government furnished remote client devices that return from international travel cannot connect to information systems and services without

having been scanned for malware, unauthorized executable code, and other unauthorized changes; and

- (f) Ensure Government furnished remote client devices are sanitized according to SP 800-88 Revision 1 requirements.
- h. System Owners of remote client devices that are used for international travel will:
 - (1) Develop threat models and risk assessments based on risks of using such devices in foreign countries. These assessments will be:
 - (a) Reviewed at least annually and updated as necessary; and
 - (b) Shared with system owners of remote access methods and information systems that allow remote access from foreign locations.
 - (2) Use the results of risk assessments to implement security controls and maintain secure baseline configurations for their client devices that are taken to foreign countries; and
 - (3) Document in the system security plans (SSP) the assumptions and limitations, security controls, maintenance requirements, and user access and privileges permitted when using such devices in foreign locations. This information will be reviewed at least annually and updated as necessary.
- i. System, Database, and Network Administrators will:
 - (1) Comply with all Federal and Departmental requirements for configuring and updating remote client devices prior to international travel according to security requirements and controls for the expected travel destinations; and
 - (2) Provision remote client devices with the applicable country label and add the MDM profile.
- j. Supervisors will:
 - (1) Ensure personnel receive appropriate specialized remote access and remote client device security training prior to departing on international travel; and
 - (2) Approve personnel to bring Government furnished remote client devices and information on international travel only when necessary to meet mission requirements.
- k. Users will:
 - (1) Comply with all Departmental requirements regarding:
 - (a) The proper use and protection of remote client devices, removable media, and encrypted containers while on international travel;

- (b) Obtaining approval to take and use Government furnished remote client devices and Government information (particularly CUI) while on international travel; and
 - (c) The proper use, storage, and transport of Government information and CUI while traveling and while in foreign locations.
- (2) Obtain foreign travel security and threat awareness information prior to international travel; and
 - (3) Promptly report lost or stolen remote client devices, as well as removable media containing CUI or Government information of any type.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

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

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

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

8. POLICY EXCEPTIONS

- a. All USDA agencies and staff offices are required to conform to this policy. If a specific policy requirement cannot meet a specific 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 standard operating procedure (SOP) by the Compliance and Policy Branch, [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1.

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

9. INQUIRIES

Address inquiries concerning this DR to 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, Committee on National Security Systems Instruction ([CNSSI 4009](#)), *Committee on National Security Systems (CNSS) Glossary*, April 6, 2015

Department of State, [Travel Advisories](#)

Department of State, [Travel to High-Risk Areas](#)

[Executive Order 13526](#), *Classified National Security Information*, December 29, 2009

[Executive Order 13556](#), *Controlled Unclassified Information*, November 4, 2010

Federal Information Security Modernization Act of 2014 ([FISMA](#)), 44 United States Code (U.S.C.) §3551, et seq., December 18, 2014

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

Fraud and related activity in connection with identification documents, authentication features, and information, [18 U.S.C. 1028\(d\)\(7\)](#), 2010

Government Accountability Office (GAO), [GAO-12-757](#), *Information Security Better Implementation of Controls for Mobile Devices Should Be Encouraged*, September 2012

NARA, CUI [Registry – Categories and Subcategories](#)

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

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

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

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

NIST, [SP 800-114 Revision 1](#), *User's Guide to Telework and Bring Your Own Device (BYOD) Security*, July 2016

NIST, [SP 800-122](#), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010

NIST, [SP 800-124 Revision 1](#), *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013

NIST, [SP 800-125](#), *Guide to Security for Full Virtualization Technologies*, January 2011

NIST, [SP 800-171 Revision 1](#), *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, December 2016 includes updates as of February 20, 2018

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

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

OMB, Memorandum [M-11-27](#), *Implementing the Telework Enhancement Act of 2010: Security Guidelines*, July 15, 2011

OMB, Memorandum [M-17-12](#), *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017

OMB, Memorandum [M-19-02](#), *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*, October 25, 2018

[Telework Enhancement Act of 2010](#), 5 U.S.C. §6501, et seq., (2010)

United States Atomic Energy Act 1954, as Amended, [Public Law 114-92](#), Enacted November 25, 2015

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

USDA, [CAPE-SOP-004](#), *USDA Six Step Risk Management Framework (RMF) Process Guide*, Revision 3.0, December 7, 2016

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

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

USDA, [DM 3530-005](#), *Encryption Security Standards*, February 17, 2005

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

USDA, [DR 3505-003](#), *Access Control for Information and Information Systems*, February 10, 2015

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

USDA, [DR 3540-003](#), *Security Assessment and Authorization*, August 12, 2014

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

USDA, DR 35xx-xxx, *Scanning and Remediation of Configuration and Patch Vulnerabilities*, forthcoming

USDA, [DR 3575-002](#), *System and Information Integrity*, August 16, 2018

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

USDA, DR 35xx-xxx, *Bring Your Own Device*, forthcoming

USDA, DR 3xxx-xxx, *Controlled Unclassified Information*, forthcoming

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

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

USDA, [DR 5400-007](#), *Text Messaging While Driving*, September 7, 2010

USDA, OHS, [Foreign Travel Information](#)

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)

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)

Client Device.

- a. A system used by a remote worker to access an organization's network and the systems on that network. (Source: NIST SP 800-46 Revision 2)
- b. Two categories of client devices defined by NIST and used in this policy: PCs (e.g., desktops and laptops) and mobile devices (e.g., smartphones and tablets).
- c. See related terms "mobile device" and "personal computer."

Container. The file used by a virtual disk encryption technology to encompass and protect other files. (Source: NIST SP 800-111)

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 Executive Order 13526 or the *United States Atomic Energy Act 1954*, as Amended. (Source: Executive Order 13556)

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)

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 System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: OMB Circular A-130)

Malware. A program that is covertly inserted into a system or another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the

confidentiality, integrity, or availability of the victim's data, applications, or operating system. (Source: NIST SP 800-83 Revision 1)

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

Mobile Work. Work which is characterized by routine and regular travel to conduct work in customer or other worksites as opposed to a single authorized alternative worksite. Examples include site audits, site inspections, investigations, property management, and work performed while commuting, traveling between worksites, or on temporary duty. Mobile work is not considered telework; however, mobile workers may be eligible to participate in telework, as applicable. (Source: DR 4080-811-02)

Need-to-Know. Decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties. (Source: CNSSI 4009)

Organization-Controlled Device. A telework client device controlled by a U.S. Government organization (e.g., Government furnished equipment, Government furnished device). Client devices in this category are usually acquired, configured, and managed by the organization. (Source: Adapted from NIST SP 800-46 Revision 2)

Personal Computer (PC). A desktop or laptop computer. (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 SP 800-122)

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 800-88 Revision 1)

Quarantine. Isolation for devices or files that contain, or may contain, malware for future disinfection or examination. (Source: Adapted from NIST IR 7298 Revision 2)

Remote Access. The ability for an organization's users to access its non-public computing resources from external locations other than the organization's facilities. (Source: CNSSI 4009)

Remote Access Method. Mechanisms that enable users to perform remote access. There are four types of remote access methods: tunneling, portals, remote desktop access, and direct application access. (Source: Adapted from NIST SP 800-46 Revision 2)

Removable Media. Portable data storage medium that can be added to or removed from a computing device or network. Examples include, but are not limited to: optical discs; external/removable hard drives; external/removable Solid State Disk (SSD) drives; magnetic/optical tapes; flash memory devices; flash memory cards; and other external/removable disks. (Source: Adapted from CNSSI 4009)

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)

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)

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)

Telework. The term ‘telework’ or ‘teleworking’ refers to a work flexibility arrangement under which an employee performs the duties and responsibilities of such employee’s position, and other authorized activities, from an approved worksite other than the location from which the employee would otherwise work. Telework may be authorized for an entire duty day or a portion of one. Telework does not include the following:

- (1) Work performed while on official travel status;
- (2) Work performed while commuting to/from work; or
- (3) Mobile work. (Source: DR 4080-811-002)

Telework Client Device. A PC or mobile device used by a teleworker for performing telework—sometimes referred to as telework device. (Source: NIST SP 800-46 Revision 2)

Third-Party-Controlled Device. A client device controlled by a contractor, business partner, or vendor. These client devices are controlled by the remote worker’s employer, who is ultimately responsible for securing the client devices and maintaining their security. (Source: Adapted from NIST SP 800-46 Revision 2)

Virtual Disk Encryption. The process of encrypting a container, which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided. (Source: NIST SP 800-111)

Virtual Environment. All forms of virtual remote access components such as virtual machine, virtual device, virtual mobile device, virtual device infrastructure, virtual mobile infrastructure, and encrypted container that ensures Federal information is under USDA control and encrypted when necessary.

Virtual Private Network. A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks. (Source: NIST SP 800-46 Revision 2)

APPENDIX C

ACRONYMS AND ABBREVIATIONS

AO	Authorizing Official
ASOD	Agriculture Security Operations Division
BYOD	Bring Your Own Device
CAPE	Compliance, Audit, Policy, and Enforcement
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
COR	Contracting Officer's Representative
CSIRT	Computer Security Incident Response Team
CUI	Controlled Unclassified Information
DM	Departmental Manual
DR	Departmental Regulation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FOUO	For Official Use Only
GAO	Government Accountability Office
IR	Interagency Report
ISC	Information Security Coordinator
ISSPM	Information Systems Security Program Manager
MDM	Mobile Device Management
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OHS	Office of Homeland Security
OMB	Office of Management and Budget
PC	Personal Computer
PDSD	Personnel and Document Security Division
PII	Personally Identifiable Information
PIV	Personal Identity Verification
RMF	Risk Management Framework
SBU	Sensitive but Unclassified
SIM	Subscriber Identity Module
SOP	Standard Operating Procedure
SP	Special Publication
SSD	Solid State Disk
SSI	Sensitive Security Information
SSP	System Security Plan
U.S.	United States
U.S.C.	United States Code
USDA	United States Department of Agriculture
VPN	Virtual Private Network
Wi-Fi	A trademark of the Wi-Fi Alliance

WPA2 Wi-Fi Protected Access 2