

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

DEPARTMENTAL REGULATION	NUMBER: DR 3580-004
SUBJECT: Securing Remote Access to USDA Information Systems and Client Devices	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. Special Instructions/Cancellations	2
3. Background	3
4. Scope	4
5. Policy	5
6. Securing USDA Information	6
7. Remote Access Infrastructure	8
8. Remote Client Device Security	13
9. Physical Security Protection	16
10. Roles and Responsibilities	17
11. Penalties and Disciplinary Actions for Non-Compliance	20
12. Policy Exceptions	20
13. Inquiries	21
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 systems with secure devices.
- b. It is USDA's policy to comply with Federal requirements to establish, implement, and enforce a policy on USDA information systems that facilitate remote access and devices used to access USDA information systems remotely.
- 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) Memorandum [M-11-27](#), *Implementing the Telework Enhancement Act of 2010: Security Guidelines*;
 - (8) OMB Memorandum [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 Mission Areas, agencies, and staff offices to develop and implement procedures for secure remote access to USDA information systems, and secure use of devices when used for remote access that comply with Federal and Departmental requirements.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy supersedes DR 3580-003, *Mobile Computing*, dated September 24, 2013.
- b. This policy is effective immediately and remains in effect until it is superseded or expires.
- c. All Mission Areas, agencies, and staff offices will align their client device, remote access, and mobile work procedures with this DR and DR 4080-811-002 within 6 months of the publication date.
- d. This DR uses the term “remote client device” in place of NIST’s “telework client device.”

Two categories of client devices defined by NIST and used in this policy are:

- (1) Personal Computers (PC) (e.g., desktops and laptops); and

- (2) Mobile devices (e.g., smartphones and tablets).

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

USDA desktop computers used only within USDA facilities to access USDA information systems do not need the same security requirements as remote client devices that access USDA information systems remotely. Section 5c addresses USDA desktop requirements when used in locations other than USDA facilities. Devices used both inside and outside of USDA facilities must meet configuration requirements in this DR.

- e. This policy uses the following terms as stated below:
 - (1) “Controlled Unclassified Information” (CUI) replaces and encompasses all previous terms and labels for sensitive information, such as, for official use only (FOUO) and sensitive but unclassified (SBU). The National Archives and Records Administration (NARA) [CUI Registry - Categories and Subcategories](#) defines 23 categories of CUI;
 - (2) “Domestic travel” includes travel to all 50 states and U.S. territories;
 - (3) “International travel” refers to business trips, as well as permanent duty assignments in any country, territory, or commonwealth outside of the United States and U.S. territories;
 - (4) “Virtual environment” encompasses 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; and
 - (5) “Wireless” refers to client devices, (e.g., laptops smartphones) and networking devices (e.g., access points) exchanging data through radio communication within a limited geographic area, such as an office building.

3. BACKGROUND

- a. The USDA remote access infrastructure affords personnel convenient and efficient methods to use client devices to access USDA resources from remote locations. However, client devices, when used remotely (e.g., outside of the USDA physical or logical boundary protections), introduce additional risks to USDA information and information systems; therefore, these devices have additional security requirements beyond those that apply to information technology equipment operating within USDA owned, leased, or controlled physically protected areas.
- b. System owners that permit information systems to be accessed remotely through remote access infrastructure assets must safeguard USDA information from threats arising from the lack of physical security controls, the use of unsecure networks, and potentially

compromised client devices used by personnel when working remotely. Personnel using remote client devices are responsible for protecting them and knowing how, when, and where to use client devices securely.

c. There are four remote access methods:

- (1) Tunneling: virtual private network (VPN);
- (2) Application Portal: such as virtual desktop infrastructure (VDI), virtual mobile infrastructure (VMI), and bootable secure operating system;
- (3) Direct Application Access: such as Web mail, timecard system; and
- (4) Remote Desktop Access: such as used by Helpdesk/Tech Support for administrative access.

d. There are four client device ownership categories:

- (1) Government furnished equipment (GFE), also referred to as organization-controlled devices;
- (2) Personally owned devices, typically referred to as BYOD;
- (3) Third-party-controlled devices, which includes devices owned or controlled by contractors, business partners, and vendors; and
- (4) Unknown devices, which includes client devices owned or controlled by hotels, kiosks, friends, or family members.

Note: Third-party-controlled devices are permitted to access USDA information systems when permitted by contract (see Sections 5a and 5b). Unknown devices are never permitted to access USDA information systems (see Section 8k).

4. 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 virtual environments; 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 upon other USDA information security policies that address application and device security requirements; however, this DR emphasizes identifying security requirements to enable individuals to remotely access USDA information systems in accordance with [DR 4080-811-002](#), *Telework Program*. This policy addresses the security of systems that implement remote access methods, USDA information systems that allow remote access, and devices that are used for remote access.
- c. This policy complements other information security policies, programs, and procedures including:
 - (1) The following DRs and Departmental Manuals (DM):
 - (a) [DM 3530-005](#), *Encryption Security Standards*;
 - (b) [DR 3505-003](#), *Access Control for Information and Information Systems*;
 - (c) [DR 3520-002](#), *Configuration Management*;
 - (d) [DR 3575-002](#), *System and Information Integrity*; and
 - (e) [DR 3640-001](#), *Identity, Credential, and Access Management*.
 - (2) The following future DRs:
 - (a) DR 35xx-xxx, *Scanning and Remediation of Configuration and Patch Vulnerabilities*, forthcoming; and
 - (b) DR 35xx-xxx, *Bring Your Own Device*, forthcoming.
- d. Users should comply with [DR 5400-007](#), *Text Messaging While Driving*, September 7, 2010, which provides safety guidance about the use of GFE and driving.
- e. Nothing in this policy will alter the requirements of DR 4080-811-002 that defines approved worksites for USDA, when those worksites may be used, and the conditions under which they may be used.
- f. 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.

5. POLICY

- a. Requirements and security controls for client devices will be included in all contracts and agreements with third parties including contractors, business partners, and vendors that require access to USDA information systems.

- b. Mission Areas, agencies, and staff offices that allow third-party-controlled devices to access USDA information systems or services will have contract requirements specifying that third-party-controlled devices implement the same or better security controls as Government furnished client devices.
- c. Government furnished desktop computers accessing or storing USDA information remotely will have the same information storage restrictions, configuration, operational, and sanitization requirements as laptops.
- d. Mission Areas, agencies, and staff offices will develop, implement, and maintain procedures for remote access, remote client devices, and virtual environments that:
 - (1) Include security practices in all phases of remote access infrastructure and remote client device life cycles;
 - (2) Incorporate remote access procedures into business continuity plans;
 - (3) Integrate with other security processes such as risk management, security assessments, continuous monitoring, incident management, and system error handling;
 - (4) Integrate with vulnerability management processes and requirements such as vulnerability remediation, application of security-relevant software updates (e.g., patches and anti-malware signatures), and system configuration hardening;
 - (5) Maintain an active inventory of remote client devices, virtual devices, encrypted containers issued, and the user assigned to each device or virtual device; and
 - (6) Implement monitoring capabilities to maintain current, complete, and accurate configuration baselines and to detect and respond to unauthorized changes or anomalous characteristics occurring over remote access sessions.

6. SECURING USDA INFORMATION

- a. Mission Areas, agencies, and staff offices will:
 - (1) Encrypt all Federal information stored on remote client devices with NIST certified cryptographic modules and comply with DM 3530-005;
 - (2) Store CUI only on Government furnished client devices and encrypted containers created as components of a USDA information system that has authority to operate; and
 - (3) Ensure that BYOD, and third-party-controlled devices permitted to access USDA information systems:
 - (a) Are prohibited from storing personally identifiable information (PII); and

- (b) Are permitted to store other categories of CUI only:
 - 1 After completion of a risk assessment approved by a Chief Information Security Officer (CISO), Information Systems Security Program Managers (ISSPM), or other individual authorized to accept risk for the organization; and
 - 2 When stored in an encrypted container.
- (4) Minimize the downloading and storage of CUI on remote client devices to the least amount of information needed to perform official business; and
- (5) Train employees on the required methods to protect CUI and PII information.
- b. All CUI residing on remote client devices will be sanitized in accordance with NIST, [SP 800-88 Revision 1](#), *Guidelines for Media Sanitization*:
 - (1) Within 30 days of when the information is no longer needed;
 - (2) Prior to vendors conducting maintenance if those vendors are not authorized to access CUI;
 - (3) Within 30 days of when the user no longer requires use of the device and it will be disposed of; or
 - (4) Prior to reassigning the device to another user.
- c. Mission Areas, agencies, and staff offices that allow BYOD and third-party-controlled devices to store Federal information will sanitize Federal information in accordance with SP 800-88 Revision 1, using the functionality of mobile device management (MDM) or other software, without affecting personal or third-party information or software.
- d. Mission Areas, agencies, and staff offices will document in the System Security Plans (SSP) of USDA information systems that:
 - (1) Allow CUI to be extracted from, stored on, or transferred to remote client devices will be documented with the security controls that:
 - (a) Enforce the encryption and logging of CUI; and
 - (b) Require sanitization of CUI, using the clear method as described in NIST SP 800-88 Revision 1, Section 5, within 90 days of the CUI being introduced to the remote client device or verify its use is still required.
 - (2) Allow access to but prohibit computer readable extracts of CUI, including the methods implemented to prevent extractions of CUI.

Note: Additional SSP documentation requirements are also in section 7r.

- e. Public printers will not be used to print CUI.

7. REMOTE ACCESS INFRASTRUCTURE

Remote access consists of any connection to the USDA network or access to USDA non-public information resources from outside of a USDA owned or operated network infrastructure.

- a. Mission Areas, agencies, and staff offices will develop threat models for:
 - (1) Each of the remote access methods;
 - (2) Each ownership category of remote client device, based on the party that is responsible for the security of the device; and
 - (3) Remote access locations such as home, third-party sites, domestic, and international destinations.
- b. Supporting and supported organizations will share threat models in order to:
 - (1) Facilitate the development of organizationally independent threat models; and
 - (2) Facilitate the establishment of interdependent risk assessments.
- c. Risk assessments will identify the risks associated with remote access to each USDA information system or service.
- d. Tiered remote access guidance limits risk by permitting the most controlled devices to have more access to USDA information systems and services, while devices with less control have less or no access. For example, one tier of remote access guidance may allow Government issued mobile devices to access many resources, while another tier may allow BYOD mobile devices to access only email.
- e. Mission Areas, agencies, and staff offices will develop tiered remote access guidance based on assessments of risk to USDA information systems or services.
- f. Tiered access to USDA information systems will restrict remote access based on the risks associated with:
 - (1) The remote access method;
 - (2) The types of remote client devices permitted to be used, specified separately for each of the security ownership categories:
 - (a) GFE;
 - (b) BYOD;

- (c) Third-party-controlled; and
 - (d) PC owned by USDA personnel.
- (3) The sensitivity of the information, resource, or service;
 - (4) The location where the remote access is performed such as:
 - (a) The user's home;
 - (b) Domestic travel locations;
 - (c) International travel locations not identified as high risk; and
 - (d) International travel locations identified as high risk in [DR 3580-005](#), *Securing Client Devices for International Travel*.

Note: Risk decisions informed by the classified information provided by the High Risk Travel Briefings must not be documented in unclassified SSPs. However, the information is used to assess whether the remote access method and a remote client device used in a high risk country sufficiently protects USDA information systems from unauthorized access.

- (5) The confidence in security policy compliance.
- g. Mission Areas, agencies, and staff offices will reassess, and update if necessary, their tiered remote access guidance at least annually based on:
 - (1) The threats to remote access methods and remote client devices used by the Mission Area, agency, or staff office;
 - (2) Available security controls;
 - (3) Major changes to remote access technologies; and
 - (4) Remote client device capabilities.
 - h. All remote access methods will:
 - (1) Use USDA approved enterprise solutions when available and appropriate;
 - (2) Enforce information transfers using information paths designated by the Mission Area, agency, or staff office;
 - (3) Assess and verify the security posture of the following before granting access to USDA information systems:
 - (a) Government furnished remote client devices attempting to connect; and

- (b) Encrypted containers.
- (4) Automatically deny connection attempts from remote client devices that do not meet USDA security requirements including:
 - (a) GFE and encrypted containers that do not comply with secure configuration baseline requirements;
 - (b) Devices that have been tampered with (i.e., jailbroken or rooted);
 - (c) User accounts or client devices that have not been provisioned to connect to USDA information systems; and
 - (d) Users that are not authorized to work remotely.
- (5) Authenticate each individual authorized for remote access in accordance with DR 3640-001, *Identity, Credential, and Access Management*;
- (6) Only allow access to approved resources; and
- (7) Use an encrypted VPN in compliance with DR 3505-003 to transmit all USDA information between USDA information systems and remote client devices.
- i. Remote access tunnel systems will:
 - (1) Only be accessible through firewalls;
 - (2) Be placed in the network where network traffic:
 - (a) Is best protected from known threats; and
 - (b) Can be monitored for malicious or anomalous activity.
 - (3) Enforce the remote access policies and associated procedures before any remote access traffic is permitted access to internal resources;
 - (4) Not run on the same physical host as other services and applications unless a risk assessment is performed and mitigating security controls are implemented;
 - (5) Be configured to enforce remote access only to USDA information systems or services specifically authorized for remote access; and
 - (6) Be manageable from trusted hosts by authorized administrators.
- j. Remote Desktop Access methods will:
 - (1) Only be used by authorized USDA technical support personnel; and
 - (2) Require the user to grant permission for each remote access request.

- k. Direct Application Access methods will:
 - (1) Ensure direct application servers are located at the USDA network perimeter or in a public-facing cloud, and not within the internal network; and
 - (2) Limit access to lower risk applications, such as Web mail when direct application access servers are accessed from the Internet.
- l. Application Portal methods will:
 - (1) Only allow remote access to the following remote client devices:
 - (a) Government furnished client devices; and
 - (b) BYOD or third-party-controlled client devices configured with remote access client software that establishes a virtual environment such as VMI, VDI, or bootable compact disc (CD) (or read-only flash drives); and
 - (2) Based on the risk assessment, implement a process to sanitize CUI temporarily stored on portal servers when the data is no longer needed.
- m. Mission Areas, agencies, and staff offices will implement centrally managed:
 - (1) MDM solutions to:
 - (a) Determine whether a mobile device has been jailbroken or rooted;
 - (b) Enforce a secure baseline configuration and access control requirements on Government furnished mobile devices and encrypted containers, to reflect technology, policy, or security changes;
 - (c) Monitor and report unauthorized application installations or modifications to a configuration; and
 - (d) Audit access to a Government furnished mobile device or encrypted container.
 - (2) Mobile application management (MAM) solutions to maintain baseline configurations for enterprise applications on Government furnished mobile devices and encrypted containers.
- n. Mission Areas, agencies, and staff offices will ensure that internal resources approved for remote access:
 - (1) Are hardened against external threats;
 - (2) Limit access to the minimum resources necessary to support personnel working remotely; and

- (3) Use remote access methods approved by the Mission Area Assistant Chief Information Officer (CIO).
- o. Prior to allowing the use of remote client devices, Mission Areas, agencies, and staff offices will specify in SSPs the types of information that may be stored on the devices and how to sanitize the information when no longer needed.
- p. Mission Areas, agencies, and staff offices will develop and implement a vetting process, in accordance with DR 3520-002, and NIST [SP 800-163](#), *Vetting the Security of Mobile Applications*, to test and evaluate mobile applications (apps) and software programs prior to their installation on Government furnished mobile devices and encrypted containers.
- q. Mission Areas, agencies, and staff offices that allow BYOD or third-party-controlled client devices to be used within USDA facilities will:
 - (1) Implement a separate, externally dedicated network on USDA's demilitarized zone for such devices;
 - (2) Require pre-approval for each client device to connect to the dedicated network in accordance with DR 3520-002;
 - (3) Require such devices to use USDA's Internet facing remote access methods to gain access to USDA internal resources;
 - (4) Not permit more access to USDA resources when working remotely than the users would normally have; and
 - (5) Implement security configurations and monitoring commensurate with remote access segments.
- r. Mission Areas, agencies, and staff offices will document in the SSP:
 - (1) The internal resources that are authorized to be accessed remotely and how they are hardened against external threats;
 - (2) The underlying security architecture supporting the remote access methods;
 - (3) The methods for remote access permitted to access USDA information systems;
 - (4) The types of remote client devices permitted for each form of remote access;
 - (5) The level or type of access and associated privileges granted to each role authorized to work remotely;
 - (6) The provisioning and de-provisioning process for remote access;
 - (7) The procedures used to administer USDA information systems and resources remotely, which include applying patches and making security configuration

changes approved through the Mission Area, agency, or staff office Configuration Control Board (CCB);

- (8) The procedures used to maintain security configurations for USDA information systems and resources accessed remotely commensurately with those internal to the USDA computing environment;
- (9) The conditions, limitations, and usage restrictions for remote access, such as:
 - (a) Types of devices that the remote access infrastructure does not support;
 - (b) Client devices not registered and approved to access USDA information resources; and
 - (c) Ports and protocols not authorized by the Mission Area, agency, or staff office to be active during remote access sessions (e.g., Bluetooth object exchange file sharing or file transfer capabilities).

Note: Documentation requirements for the SSP can also be found in Section 6d.

- s. Mission Areas, agencies, and staff offices will review, and update if necessary, the risk mitigation strategies and the SSP at least annually to reflect changes in technologies or the threat environment.
- t. Mission Areas, agencies, and staff offices will develop and deliver secure remote access training and materials that address specialized training and guidance for administrative staff who manage remote access servers, connections, and client devices and use privileged accounts while working remotely.

8. REMOTE CLIENT DEVICE SECURITY

- a. Mission Areas, agencies, and staff offices will ensure that all USDA owned and managed remote client devices, virtual environments, and associated data are subject to electronic discovery (eDiscovery) for business purposes. In some cases, agencies or staff offices may physically collect the remote client devices to retrieve data and return the device to the user.
- b. Mission Areas, agencies, and staff offices will ensure that all Government furnished remote client devices, secure virtual machines, and encrypted containers that connect to Federal information systems are under configuration control and hardened to comply with configuration checklists.
- c. Mission Areas, agencies, and staff offices will ensure that mobile devices meet the following requirements prior to being issued to users:
 - (1) All compatible Government furnished mobile devices have MDM or MAM client software installed; and

- (2) The MDM or MAM software is implemented correctly, operating as intended, and producing the desired outcome.
- d. All compatible Government furnished remote client devices and encrypted containers will comply with DR 3520-002, *Configuration Management*, DR 3575-002, *System and Information Integrity*, and NIST, [SP 800-111](#), *Guide to Storage Encryption Technologies for End User Devices*.
- e. Mission Areas, agencies, and staff offices will allow users to enable and disable communication services in accordance with DR 3505-003.
- f. Prior to providing Government furnished remote client devices to personnel, the devices will be configured to:
 - (1) Disable Bluetooth communications;
 - (2) Disable Bluetooth advertising and broadcast functionality;
 - (3) Disable Bluetooth auto pairing functionality;
 - (4) Implement the strongest Bluetooth security and encryption modes supported by the device;
 - (5) Implement firewall software, when compatible; and
 - (6) Enable remote sanitization of all information stored on the device.
- Note: Bluetooth accessories such as keyboards, mice, and earphones are permitted, but the protocol must be disabled (turned off) when the accessories are not in use.
- g. Lost or stolen Government furnished remote client devices will be remotely sanitized to the extent that remote sanitization is supported on the device; and if later found, they will be sanitized in accordance with SP 800-88 Revision 1.
- h. Mission Areas, agencies, and staff offices will ensure backup procedures:
 - (1) For remote client devices to have commensurate security protections for the sensitivity level of the information stored on the remote client device; and
 - (2) Are provided to users of remote client devices.
- i. Mission Areas, agencies, and staff offices will ensure:
 - (1) That help is available during business hours to respond to questions or concerns regarding remote access security for individuals working remotely; and
 - (2) Users are made aware of how to request help.
- j. Mission Areas, agencies, and staff offices will:

- (1) Ensure that personnel sign Agriculture Department [\(AD\)-3051](#), *Acceptable Use Policy Agreement* (AUPA), and either [AD-3052](#), *Rules of Behavior* (ROB) or other Department approved rules of behavior for remote access prior to being assigned a remote client device. These forms are available electronically on the [USDA Departmental Forms Management Website](#). Mission Areas, agencies, and staff offices are permitted to add more stringent requirements to the baseline AUPA or ROB agreements, but they may not weaken the baseline requirements described in AD-3051 and AD-3052;
- (2) Ensure personnel using Government furnished remote client devices are informed that:
 - (a) Personal information and related transmissions, including but not limited to: text messages, digital photos, and files, (including personal files such as tax documents, wage statements, and health data) stored on such devices, may be monitored, intercepted, searched, recorded, archived, deleted, or seized by the Department; and
 - (b) The Department will not be responsible for recovering or restoring personal data stored on Government furnished devices.
- (3) Formally document user acceptance of USDA remote client devices with appropriate device inventory information such as serial number and device name; and
- (4) Ensure personnel using a Government furnished remote client device follow USDA de-provisioning requirements upon loss of eligibility to work remotely.
- k. Personnel will not use unknown devices for conducting official business. See Section 3d(4) for examples of unknown devices.
- l. When remotely accessing information systems, personnel will only store USDA information on USDA information systems that have authority to operate including:
 - (1) Government furnished client devices;
 - (2) Secure virtual machines and encrypted containers created as components of USDA information systems; and
 - (3) Cloud systems under contract by or with USDA.
- m. Mission Areas, agencies, and staff offices will encourage users to configure their home wireless and wired networks securely in accordance with Chapter 4 of NIST SP 800-114 Revision 1.

9. PHYSICAL SECURITY PROTECTION

The requirements in this section apply to protecting equipment. Additional requirements for protecting remote client devices while remotely working from an international location are in DR 3580-005.

a. Users will:

- (1) Exercise due diligence and due care to protect remote client devices against loss, theft, and unauthorized access by retaining positive control of the devices at all times; and
- (2) Position remote client devices, when in use outside of secure locations, so that information displayed on screens or typed on keyboards is not easily observed by others.

b. When not using the remote client device, users will:

- (1) Keep the device within direct sight, or in a container (e.g., backpack, purse, briefcase, carry-on luggage) that is within direct sight of the user;
- (2) Not place the device in checked baggage; and
- (3) Secure the device when leaving it unattended, such as by:
 - (a) Placing the device in a hotel room safe;
 - (b) Locking the device to a desk or other similar semi-movable or immovable object;
 - (c) Placing the device in a locked office or inside a drawer or file cabinet within a Federal building or facility;
 - (d) Storing the device in the user's home; or
 - (e) Placing the device inside the locked trunk of a motor vehicle.

c. Users will maintain personal possession of identity and access control credentials (e.g., Personal Identity Verification (PIV) card) when traveling and store them separately from the associated remote client devices at other times; and

d. Users will report the loss or theft of their access control credentials or Government furnished remote client device as soon as detected to the Agriculture Security Operations Division (ASOD) Computer Security Incident Response Team (CSIRT) through the ASOD 24 Hour Hotline (866-905-6890) or via email to the Cyber mailbox (cyber.incidents@asoc.usda.gov). Personnel will also report the loss or theft of their access control credential to the USDA sponsor.

10. ROLES AND RESPONSIBILITIES

- a. The USDA CIO will:
 - (1) Provide ongoing funding and support for the Department's secure remote access capabilities; and
 - (2) Ensure cybersecurity policies governing requirements for remote access, secure use, and protection of remote client devices are developed, disseminated, and implemented.
- b. The USDA CISO will:
 - (1) Oversee and ensure compliance with Federal and Departmental cybersecurity policies and requirements applicable to remote access and the use and protection of client devices;
 - (2) Ensure remote access and secure client device capabilities are incorporated in the Department's business continuity plans and strategies;
 - (3) Provide guidance to USDA Mission Areas, agencies, and staff offices to ensure implementation of and compliance with Departmental cybersecurity requirements for remote access, secure use, and protection of client devices;
 - (4) Adjudicate requests for waivers from remote client device sanitizing requirements; and
 - (5) Ensure that user training includes techniques for secure remote access to USDA information systems and secure use and protection of client devices.
- c. The ASOD Director will coordinate the necessary actions to remotely track, purge, and disable lost or stolen remote client devices.
- d. Mission Area, agency, and staff office Authorizing Officials (AO) will:
 - (1) Be responsible for risk-based decisions regarding remote access and remote client device use;
 - (2) Adjudicate and approve only for compelling mission and operational requirements waivers that allow:
 - (a) CUI, other than PII, to be stored on BYOD or third-party-controlled devices; and
 - (b) The use of remote client devices that do not support two-factor authentication.
- e. Mission Area Assistant CIOs will:

- (1) Ensure that Mission Area Assistant CISOs and ISSPMs have adequate resources including funding, personnel, and training to implement and support the remote access infrastructure, remote client device security, and domestic travel security requirements;
 - (2) Approve remote access methods used by Mission Area, agency, or staff office information systems; and
 - (3) Ensure remote access architectures protect the Mission Area, agency, or staff office computing environment and information resources from malicious activity.
- f. Mission Area Assistant CISOs and ISSPMs will:
- (1) Ensure that threat models and risk assessments of remote access methods and remote client devices are shared with system owners of USDA information systems and services that use the remote access methods and remote client devices;
 - (2) Ensure that system lifecycle procedures (planning, development, test, and operating) of remote access methods and client devices are integrated with Departmental inventory, scanning, configuration and vulnerability management, and monitoring procedures;
 - (3) Ensure guidance for tiered remote access to USDA information systems and services is documented and based on a risk assessment of the sensitivity of remote access and the confidence in the compliance with security controls of USDA information systems, remote access methods, and remote client devices;
 - (4) Ensure processes and procedures require personnel to receive specialized training on secure remote access and secure use and protection of client devices in accordance with [DR 3545-001](#), *Information Security Awareness and Training Policy*;
 - (5) Develop processes and procedures for obtaining and using threat intelligence and risk assessments to implement secure configuration baselines; and
 - (6) Develop processes and procedures to sanitize Government furnished remote client devices using SP 800-88 Revision 1 methods.
- g. System owners of systems that implement remote access methods will:
- (1) Develop, review at least annually, and update as necessary, threat models and risk assessments of remote access methods, and share them with system owners of USDA information systems and remote client devices;
 - (2) Use the results of risk assessments to develop security controls and maintain secure baseline configurations for remote access methods;

- (3) Document in the SSPs, review at least annually, and update as necessary, the assumptions and limitations, security controls, maintenance requirements, and user access and privileges permitted of remote access methods.
- h. System owners of USDA information systems and remote client devices will:
 - (1) Develop, review at least annually, and update as necessary, remote access threat models and risk assessments of USDA information systems that allow remote access and share them with system owners of systems that implement remote access methods;
 - (2) Document in the SSPs, review at least annually, and update as necessary, the assumptions and limitations of remote access methods used, the security controls, maintenance requirements, and permitted accesses and privileges of users and support staff of the USDA information system;
 - (3) Ensure that SSPs are updated to include the requirements in Sections 6d and 7r;
 - (4) Use the results of risk assessments to implement and maintain the security controls for USDA information systems; and
 - (5) Ensure that CUI is logged, encrypted in transit and in storage, and sanitized using the clear method (or better) within 90 days of the CUI being introduced to the remote client device or verify its use is still required when allowed to be extracted and downloaded to remote client devices.
- i. System, database, and network administrators will:
 - (1) Comply with all Federal and Departmental requirements for configuring and updating the components of remote access methods and client devices; and
 - (2) Implement additional security controls, adhering to the configuration control process, for USDA information systems based on the results of remote access risk assessments.
- j. Supervisors will:
 - (1) Ensure personnel and administrators receive appropriate specialized training for secure remote access and secure use and protection of client devices;
 - (2) Approve personnel and administrators to work remotely and use client devices only after they have met all Departmental requirements; and
 - (3) Approve personnel and administrator requests for remote access to USDA information systems and services only when:
 - (a) There is a valid need to perform work remotely; and

- (b) They have met access requirements in DR 3505-003.
- k. Users who are authorized for remote access to USDA information systems will:
 - (1) Complete annual training and any required specialized security training for remote access security and secure use and protection of remote client devices prior to receiving a Government furnished remote client device;
 - (2) Never use unknown PCs or mobile devices (e.g., friends, family member, or hotel) to connect to USDA information systems;
 - (3) Comply with all Departmental requirements and ROB regarding:
 - (a) The proper use and protection of remote client devices and encrypted containers to store USDA information;
 - (b) The proper use, storage, and transport of USDA information and CUI; and
 - (c) The proper installation and use of applications on Government furnished remote client devices and encrypted containers.
 - (4) Promptly report lost or stolen client devices.

11. 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 effected 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 [Standards of Ethical Conduct for Federal Employees of the Executive Branch](#).

12. POLICY EXCEPTIONS

- a. All USDA Mission Areas, agencies, and staff offices are required to conform to this policy. In the event Mission Areas, agencies, and staff offices cannot meet a specific policy requirement as explicitly stated, a waiver may be requested. Note that an approved waiver does not bring the system into compliance with policy. Requests for waivers:

- (1) Are an acknowledgement of a system's non-compliance with policy and that an acceptable plan to remediate the weakness has been provided and will be implemented.
 - (2) Must be documented as indicated in the Departmental Standard Operating Procedure (SOP) by the Compliance and Policy Branch (CPB), [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1.
- b. Mission Areas, agencies, and staff offices will address the policy waiver request memorandum to the USDA CISO and submit the request to OIS.Outreach@wdc.usda.gov for review and decision. Unless otherwise specified, Mission Areas, agencies, and staff offices must review and renew approved policy waivers every fiscal year.

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

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

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

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

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

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 800-63-3](#), *Digital Identity Guidelines*, June 2017

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 800-124 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 800-163](#), *Vetting the Security of Mobile Applications*, January 2015

NIST, [SP 800-167](#), *Guide to Application Whitelisting*, October 2015

NIST, [SP 800-190](#), *Application Container Security Guide*, September 2017

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-04-04](#), *E-Authentication Guidance for Federal Agencies*, December 16, 2003

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

[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](#), November 25, 2015

USDA, [AD-3051](#), *Acceptable Use Policy Agreement (AUPA)*, Revised September 2013

USDA, [AD-3052](#), *Rules of Behavior (ROB)*, Revised September 2013

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

USDA, [CAPE-SOP-004](#), *USDA Six-Step Risk Management Framework (RMF) Process Guide*, Revision 3, December 7, 2016

[USDA Departmental Forms Management](#)

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

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

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

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

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

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

USDA, [DR 3300-1-B](#), *Telephone Use*, March 23, 1999

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 3545-001](#), *Information Security Awareness and Training Policy*, October 22, 2013

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

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

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 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

APPENDIX B

DEFINITIONS

Application Portal. A remote access method that consists of a portal server that offers access to one or more applications through a single centralized interface combined with portal client software that runs on a client device to access the portal. (Source: Adapted from NIST SP 800-46 Revision 2)

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, *Guide to Storage Encryption Technologies for End User Devices*)

Controlled Unclassified Information (CUI). Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government wide policies but is not classified under Executive Order 13526 or the *Atomic Energy Act*, as amended. (Source: EO 13556, *Controlled Unclassified Information*)

Defense-in-Breadth. A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement). (Source: CNSSI 4009, *Committee on National Security Systems (CNSS) Glossary*)

Defense-in-Depth. Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. (Source: 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)

Direct Application Access. A high-level remote access architecture that allows teleworkers to access an individual application directly, without using remote access software. (Source: NIST SP 800-46 Revision 2)

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, *Managing Information as a Strategic Resource*)

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, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*)

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: USDA DR 4080-811-002)

Multifactor Authentication. Authentication using two or more factors to achieve authentication. Factors include: (a) something you know (e.g., password/personal identification number (PIN)); (b) something you have (e.g., cryptographic identification device, token); or (c) something you are (e.g., biometric). (Source: NIST SP 800-53 Revision 4)

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 IR 7298 Revision 2, *Glossary of Key Information Security Terms*)

Privileged Accounts. Individuals who have access to set "access rights" for users on a given system. Sometimes referred to as system or network administrative accounts. (Source: NIST IR 7298 Revision 2)

Privileged User. A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (Source: NIST SP 800-53 Revision 4)

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)

Remote Desktop Access. A high-level remote access architecture that gives a teleworker the ability to remotely control a particular desktop computer at the organization, most often the user's own computer at the organization's office, from a telework client device. (Source: NIST SP 800-46 Revision 2)

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)

Session Locking. A feature that permits a user to lock a session upon demand or locks the session after it has been idle for a present period of time. (Source: NIST SP 800-46 Revision 2)

Split Tunneling. A VPN client feature that tunnels all communications involving the organization's internal resources through the VPN, thus protecting them, and excludes all other communications from going through the tunnel. (Source: NIST SP 800-46 Revision 2)

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)

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)

Tunneling. A high-level remote access architecture that provides a secure tunnel between a telework client device and a tunneling server through which application traffic may pass. (Source: NIST SP 800-46 Revision 2)

Unknown Device. A client device that is owned and controlled by other parties, such as a computer at hotels, and a PC or mobile device owned by friends and family. The device is labeled as “unknown” because there are no assurances regarding its security posture. (Source: Adapted from NIST SP 800-46 Revision 2)

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

Virtual Private Network (VPN). 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

AD	Agriculture Department
AO	Authorizing Official
ASOD	Agriculture Security Operations Division
AUPA	Acceptable Use Policy Agreement
BYOD	Bring Your Own Device
CAPE	Compliance, Audit, Policy, and Enforcement
CCB	Configuration Control Board
CD	Compact Disc
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CSIRT	Computer Security Incident Response Team
CUI	Controlled Unclassified Information
DM	Departmental Manual
DR	Departmental Regulation
eDiscovery	Electronic Discovery
EO	Executive Order
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
FOUO	For Official Use Only
GAO	Government Accountability Office
GFE	Government Furnished Equipment
IEEE	Institute of Electrical and Electronics Engineers
IR	Interagency Report
ISSPM	Information Systems Security Program Manager
MAM	Mobile Application Management
MDM	Mobile Device Management
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PC	Personal Computer
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
POA&M	Plan of Action and Milestones
PUB	Publication
RMF	Risk Management Framework
ROB	Rules of Behavior
SBU	Sensitive But Unclassified
SOP	Standard Operating Procedures
SP	Special Publication

SSP	System Security Plan
U.S.	United States
U.S.C.	United States Code
USDA	United States Department of Agriculture
VDI	Virtual Desktop Infrastructure
VMI	Virtual Mobile Infrastructure
VPN	Virtual Private Network