

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

|   |                                   |
|---|-----------------------------------|
| <b>DEPARTMENTAL REGULATION</b>  | NUMBER:<br>DR 3505-003            |
| SUBJECT: Access Control for Information and Information Systems           | DATE:<br>July 17, 2019            |
| OPI: Office of the Chief Information Officer, Information Security Center | EXPIRATION DATE:<br>July 17, 2024 |

| <u>Section</u>   | <u>Page</u> |
|--|-------------|
| 1. Purpose   | 2           |
| 2. Special Instructions/Cancellations                          | 2           |
| 3. Background  | 3           |
| 4. Scope   | 3           |
| 5. Policy  | 4           |
| 6. Account Management  | 4           |
| 7. Access Enforcement  | 8           |
| 8. Information Flow Enforcement                                | 8           |
| 9. Separation of Duties  | 9           |
| 10. Least Privilege  | 9           |
| 11. Unsuccessful Login Attempts                                | 10          |
| 12. System Use Notification                                    | 10          |
| 13. Concurrent Session Control                                 | 12          |
| 14. Session Lock   | 12          |
| 15. Session Termination  | 13          |
| 16. Permitted Actions without Identification or Authentication | 13          |
| 17. Remote Access  | 13          |
| 18. Wireless Access  | 14          |
| 19. Access Control for Mobile Devices and Laptops              | 15          |
| 20. Use of External Information Systems                        | 16          |
| 21. Information Sharing  | 17          |
| 22. Publicly Accessible Content                                | 17          |
| 23. Roles and Responsibilities                                 | 18          |
| 24. Penalties and Disciplinary Actions for Non-Compliance      | 21          |
| 25. Policy Exceptions  | 22          |
| 26. Inquiries  | 22          |
| Appendix A - Authorities and References                        | A-1         |
| Appendix B - Definitions                                       | B-1         |
| Appendix C - Acronyms and Abbreviations                        | C-1         |
| Appendix D - System Use Notification Banner Example            | D-1         |
| Appendix E - Discussion of Logical Access Control Terms        | E-1         |

## 1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) policy for implementing, managing, and enforcing logical access to information systems and granting accounts the least privileges necessary to carry out assigned duties or actions.
- b. It is USDA policy to comply with Federal requirements by establishing, implementing, and enforcing access control policies and procedures.
- c. This policy complies with the requirements of the *Federal Information Security Modernization Act of 2014* (FISMA), [44 United States Code \(U.S.C.\) § 3551](#), et seq., and National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication [\(FIPS PUB\) 200](#), *Minimum Security Requirements for Federal Information and Information Systems*. The access control family of controls in the NIST Special Publication [\(SP\) 800-53, Revision 4](#), *Security and Privacy Controls for Federal Information Systems and Organizations*, provide the basis for this policy.
- d. This policy serves as guidance for agencies to develop and implement access control procedures that comply with Federal and Departmental requirements.

## 2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy supersedes:
  - (1) DR 3505-003, *Access Control Policy*, February 10, 2015, in its entirety; and
  - (2) DR 3505-002, *Wireless Networking Security Policy*, August 11, 2009, in its entirety.
- b. This policy is effective immediately and remains in effect until superseded or expired.
- c. All agencies will align their access control policies and procedures with this DR within 6 months of the publication date.
- d. Terminology used in this DR is defined in Appendix B, *Definitions*, and Appendix E, *Discussion on Logical Access Control Terms*.
- e. Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) and United States Government Common Baseline (USGCB) configuration checklists are available from the NIST, [National Checklist Program Repository](#). When this DR requires application of a setting to comply with a DISA STIG setting, an equivalent setting from a USGCB checklist is also permitted, without waiver.
- f. In this DR, the terms “agency,” “agencies,” “USDA agency,” or “USDA agencies,” when used generically, will be understood to include USDA Mission Areas, agencies, and staff offices collectively, unless otherwise specified.

### 3. BACKGROUND

This policy provides guidance for developing and implementing logical access controls for USDA information systems and components of USDA information systems. Controlling individual and software access and privileges to information and information systems is required to protect USDA personnel, missions, and business processes against malicious and unauthorized activities.

### 4. SCOPE

a. This policy applies to:

- (1) All USDA agencies, employees, contractors, affiliates, interns, volunteers, and fellows who work for, or on behalf of, USDA;
- (2) All Federal information, in any medium or form, generated, collected, provided, transmitted, stored, maintained, or accessed by, or on behalf of, USDA;
- (3) All information systems or services (including cloud-based services) owned, used, or operated by USDA, USDA contractors, or other organizations on behalf of, or funded by, USDA; and
- (4) Interconnections between or among these information systems.

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

- (1) DR 3xxx-xxx, *Bring Your Own Device*, forthcoming;
- (2) DR 35xx-xxx, *Identification and Authentication*, forthcoming;
- (3) [DR 3520-002](#), *Configuration Management*, August 12, 2014;
- (4) [DR 3580-004](#), *Securing Remote Access to USDA Information Systems and Client Devices*, November 30, 2018;
- (5) [DR 3580-005](#), *Securing Client Devices for International Travel*, November 30, 2018; and
- (6) [DR 3640-001](#), *Identity, Credential, and Access Management*, December 9, 2011.

c. 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 and standards issued by the Committee on National Security Systems (CNSS), or intelligence community policies, directives, and instructions.

## 5. POLICY

- a. Agencies will develop, implement, and maintain agency processes and procedures aligned with this DR to manage access to USDA information and information systems, ensuring the procedures:
  - (1) Grant access only to individuals who have an established need-to-know and who meet the minimum interim or full background investigation requirements consistent with the system and level of access being requested;
  - (2) Include monitoring and periodic validation of accounts and privileges;
  - (3) Specify remedial actions for violations; and
  - (4) Are reviewed annually and updated, if necessary.
- b. Logical access controls must:
  - (1) Be implemented in compliance with Federal, Departmental, and, if applicable, agency policies; and
  - (2) Restrict access to USDA information, information technology (IT) resources, information systems, and their components to authorized subjects.
- c. Agencies may develop and implement information security policies that meet or exceed the corresponding Departmental policy requirements. Agency policies cannot be less stringent than Departmental policy requirements. Specific policy requirements that cannot be fully implemented require an approved waiver (see section 25, *Policy Exceptions*.)

## 6. ACCOUNT MANAGEMENT

- a. Agencies will:
  - (1) Ensure that system security plans (SSP) reference processes for authorizing accounts and assigning access privileges;
  - (2) Identify and document the account types that are permitted for each USDA information system;
  - (3) Ensure user accounts issued by USDA are managed based on user identity and position data (e.g., the user role on the information system) from an authoritative source;
  - (4) Ensure that USDA information system user account records are:

- (a) Subject to electronic discovery (ediscovery) in accordance with [DR 3090-001](#), *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*; and
    - (b) Archived in accordance with the National Archives and Records Administration (NARA) [General Records Schedule 3.2: Information Systems Security Records](#).
  - (5) Assign one or more USDA personnel to serve as the account manager and System Owner's representative for each USDA information system, with the responsibility for authorizing account actions, such as creating, modifying, disabling, and deleting accounts; and
  - (6) Establish conditions for role, account, and group membership for each USDA information system, adhering to the principles of least privilege for each.
- b. Account management processes will ensure that the system owner or designated representative verifies that:
- (1) The information provided with each account access request (including modifications) is correct and accurate;
  - (2) Federal, Departmental, and agency access requirements (including interim standards, if applicable) have been met to grant the requested access;
  - (3) If any access requirements (e.g., background investigation, position suitability or fitness) have not been met, access to the information system will not be granted, or if already granted, will be disabled;
  - (4) Requests to add or change information system user account accesses or privileges meet the requirements of the information system, as defined by the system owner; and
  - (5) Account requests are submitted promptly to:
    - (a) Create accounts, add group members, and assign access privileges;
    - (b) Modify user accounts, group memberships, and access privileges when a user's work assignment changes the type of information or information system the user needs to access; or
    - (c) Disable accounts and remove group memberships when a user transfers or terminates employment, in accordance with agency procedures.
- c. Before authorizing the requested access, account managers will:
- (1) Validate the required description and justification of each role, account, or group privilege requested;

- (2) For new user requests, verify the individual's current background investigation status (including adjudication, if applicable), background investigation type, and the date that it was completed;
  - (3) For all requests, validate that the identified background investigation:
    - (a) Meets the minimum (or interim) requirements for the system and level of access requested;
    - (b) Is still valid and does not require re-investigation or has otherwise lapsed; and
    - (c) Verify through the Office of Homeland Security (OHS) or personnel security staff, that:
      1. The full investigation has been submitted to the Office of Personnel Management (OPM) for adjudication; and
      2. If granting limited interim access to begin work pending adjudication of the required background investigation, that a fingerprint check is completed with no derogatory results, in accordance with Departmental Manual [\(DM\) 4620-002](#), *Common Identification Standard for U.S. Department of Agriculture Employees and Contractors*.
  - (4) For new users, verify that individuals have completed computer security awareness training for the current fiscal year, prior to authorizing user access, and current users complete this training annually thereafter, in accordance with [DR 3545-001](#), *Information Security Awareness and Training Policy*;
  - (5) Verify annually that individuals requesting or currently holding privileged accounts have completed any required specialized role-based training;
  - (6) Verify that individuals have formally agreed to abide by the system's rules of behavior and terms of use for the current fiscal year, both initially and annually thereafter; and
  - (7) Verify that individuals will use multifactor authentication methods identified in Section 7a(2) to access USDA information systems.
- d. Account managers will only authorize requests to create, modify, disable, or delete information system accounts or access privileges following formal authorization by the system owner, employee manager, or contracting officer's representative (COR).
- e. Agency monitoring processes will:
- (1) Include audits of all accounts, groups, and roles to ensure account management procedures produce accurate and timely changes. The objectives of the monitoring and audit activities are to:

- (a) Validate with the system owner the continued business needs for each user to access active accounts or groups and ensure that accounts and groups are disabled or removed when no longer needed; and
  - (b) Reconcile active accounts, groups, and roles with account or role requests, and immediately correct or revoke any accounts or privileges not approved through the account management process. If necessary, make corrective changes to the procedures, documentation process, or require additional process training for personnel responsible for enforcing the process.
- (2) The frequency for audits will be as follows:
  - (a) Privileged user accounts/groups each quarter (or a portion of the accounts/groups more frequently);
  - (b) Non-privileged user accounts/groups at least annually; and
  - (c) Any other accounts (e.g., shared, system, service) or groups not included in Sections 6e(2)(a) and (b), at least annually.
- f. USDA information systems with a high-impact categorization will use account monitoring capabilities to identify and alert on malicious, risky, or atypical account activity.
- g. USDA information systems with a moderate- or high-impact categorization will employ an automated mechanism in the process that provides notifications to the account manager to support the management of information system accounts and to audit account usage.
- h. All USDA information systems will employ an automated mechanism in processes that:
  - (1) Disable temporary and emergency accounts within 5 workdays of when they are no longer in use or when they have expired;
  - (2) Disable public-facing, non-USDA personnel accounts within time periods set by the agency (each information system may have a different time period);
  - (3) Disable all other inactive privileged accounts within 30 calendar days, and non-privileged accounts within 60 calendar days. Information systems with a business need to keep non-privileged accounts inactive longer will be documented in the SSP; and
  - (4) Create audit records of account creation, modification, enabling, disabling, and removal actions, and notifies the account manager of these actions.
- i. Agency procedures will require that the credentials (e.g., password) for shared accounts be changed immediately when a member of the group is removed.

- j. USDA information systems with a high-impact categorization will have a process for disabling an account and privileges within a defined amount of time that a user's access is identified as posing a significant risk to the organization, the information system, other organizations, or the Nation, based on reliable evidence or intelligence. The amount of time for disabling accounts is determined by the agency, based in part on their infrastructure and capabilities.

## 7. ACCESS ENFORCEMENT

- a. USDA information systems will employ discretionary and mandatory access enforcement mechanisms to implement access control policies to ensure that:
  - (1) Only authorized subjects may access objects in accordance with information system access control policies. For example, only authorized individuals and software components may access specific information and information resources; and
  - (2) User access to a USDA information system is authenticated using a multifactor authentication method in accordance with DR 3640-001.
- b. USDA personnel will use a Personal Identity Verification (PIV) card, PIV-Interoperable card, or PIV-derived credentials to access USDA information systems, per Office of Management and Budget (OMB) mandates. Agencies may choose to implement a multifactor authentication solution for the non-USDA workforce, in accordance with DR 3640-001.
- c. Agencies will use SSPs to identify and document system functions, privileged commands, accesses, and other specified actions that require dual authorization; and enforce the dual authorization controls for those actions.

## 8. INFORMATION FLOW ENFORCEMENT

Information systems with moderate- or high-impact categorization will implement information flow control measures to:

- a. Enforce where and how information is allowed to travel within an information system and between interconnected information systems;
- b. Enforce remote access restrictions;
- c. Encrypt sensitive Controlled Unclassified Information (CUI) such as personally identifiable, export controlled, and other protected information from being transmitted as cleartext; and
- d. Prevent unauthorized communication between designated sources and destinations (e.g., individuals, devices, networks).

## 9. SEPARATION OF DUTIES

Agencies will implement the following requirements for information systems categorized as moderate- or high-impact:

- a. Document critical functions or privileged actions that require two or more individuals to implement;
- b. Separate duties to reduce the potential risks of any one individual abusing their authorized privileges for malicious purposes, by limiting the range of privileged actions an individual can perform unilaterally;
- c. Enforce information system access authorizations to separate duties for mission functions and information system support functions; and
- d. Ensure that privileged users permitted to manage access control functions cannot alter audit functions or audit records.

## 10. LEAST PRIVILEGE

- a. Individuals and system processes will have only the minimum privileges necessary to accomplish their assigned tasks.
- b. USDA information systems categorized as moderate- or high-impact will implement the principles of least privilege, ensuring that:
  - (1) Principles of least privilege are applied throughout the information system lifecycle (e.g., development, implementation, operational, and disposal phases);
  - (2) Privileged users permitted to access security functions in hardware, software, or firmware, and security relevant information will use non-privileged accounts or roles when accessing non-security features;
  - (3) Privileged accounts and groups are only used to perform privileged job functions;
  - (4) USDA information systems create audit records when a privileged command is performed, or a privileged account makes a security-related change to a USDA information system, such as creating an account or group, assigning roles and privileges to an account or group, or changing account or group privileges; and
  - (5) Configuration settings in USDA information systems prevent non-privileged users and accounts from executing privileged functions, including disabling, circumventing, or altering security safeguards and countermeasures, such as performing system integrity checks or cryptographic key management activities.
- c. For USDA information systems with a high-impact categorization, agencies will:

- (1) Only authorize remote network access to privileged commands for compelling operational needs;
- (2) Document the specific privileged commands authorized to be executed remotely; and
- (3) Provide the rationale for each authorized circumstance.

## 11. UNSUCCESSFUL LOGIN ATTEMPTS

- a. USDA information systems will use the most current DISA STIG settings to:
  - (1) Limit the number of unsuccessful login attempts at either the operating system level, the application level, or both; and
  - (2) Set time limits for the maximum consecutive invalid login attempts.
- b. When the maximum number of consecutive unsuccessful login attempts is exceeded during the specified timeframe:
  - (1) The account, application, or client device will automatically lock and remain locked for the time specified by the DISA STIG setting or until released by an administrator; and
  - (2) Agencies may establish a process to manually unlock accounts prior to the expiration of the lockout period after sufficient user identification has been established.

Note: The PIV issuance office manages the settings and recovery process for PIV credentials; therefore, settings related to PIV credentials are outside the scope of this policy.

- (3) USDA mobile devices will be configured to purge information stored on them:
  - (a) Unless the devices access network resources from a remote location via the USDA virtual private network (VPN) and those devices employ the same controls as those applied to local devices; and
  - (b) The devices are protected with sufficiently strong encryption mechanisms.

## 12. SYSTEM USE NOTIFICATION

- a. USDA information systems will display a USDA-approved notification banner at logon before granting individuals access to information systems owned by, or operated on behalf of, USDA. An example of a notification banner, approved by the Office of the General Counsel (OGC), is in Appendix D.

- b. The notification banner will remain on the screen until the individual acknowledges the usage conditions and takes explicit action to log on to the USDA information system.

Note: Information systems accessible through single sign-on sessions (e.g., SharePoint) may not need to display an additional notification banner.

- c. The banner will provide privacy and security notices consistent with requirements in applicable Federal laws, EOs, directives, policies, regulations, standards, and other guidance.
- d. The notification banner will inform the user that:
  - (1) They are accessing a U.S. Government information system;
  - (2) Usage of the information system may be monitored, recorded, and subject to audit by the U.S. Government and that users should have no expectation of privacy;
  - (3) Unauthorized use of U.S. Government information systems is prohibited and subject to criminal and civil penalties;
  - (4) Use of the system indicates consent to monitoring and recording; and
  - (5) Proceeding to the login screen constitutes the individual's acceptance of all terms and conditions in the banner.
- e. Agencies will configure systems to deny access to any individual who refuses to accept the terms and usage conditions presented in the banner.
- f. For publicly accessible USDA information systems:
  - (1) Agencies may define additional conditions for displaying a notification banner;
  - (2) The information system will display a public use notification banner before granting further access to the information system; and
  - (3) The notification banner will include:
    - (a) A statement that the user is accessing a U.S. Government information system;
    - (b) System use information and specified usage conditions;
    - (c) A description of authorized uses of the system; and
    - (d) Notice of the U.S. Government's right to monitor, record, or audit activities on the system, consistent with privacy accommodations for such systems, and citations to relevant governing authorities.
- g. Notification banners that deviate from the example in Appendix D must be submitted to the USDA OGC for approval prior to implementation.

### 13. CONCURRENT SESSION CONTROL

This control addresses concurrent sessions on a single information system (with a high-impact categorization). It does not address concurrent sessions by a single user to multiple information systems.

USDA information systems with a high-impact categorization will:

- a. Prevent non-privileged user accounts from logging into more than one concurrent privileged session;
- b. Prevent non-privileged user accounts from logging into more than two concurrent non-privileged sessions; and
- c. Permit privileged user accounts to concurrently login to no more than one privileged and two non-privileged sessions.

### 14. SESSION LOCK

Information systems typically implement session locks at the operating system level using screen savers; however, applications can also provide session locking capabilities. Users should only use session locks for short periods of inactivity and log off the system for long periods, such as at the end of the workday.

- a. USDA information systems will be configured to ensure that after the DISA STIG-specified timeframe of inactivity, an information system or client device automatically initiates a session lock to prevent further access.
- b. Agencies will either require individuals to initiate a session lock, such as a screen lock, when they leave their client device unattended or agency-owned client devices to initiate a session lock when the user removes the PIV card from the client device.
- c. USDA information systems and client devices will maintain the session lock until the user re-authenticates to the information system or device using established USDA identification and authentication procedures in accordance with DR 3640-001.
- d. During a session lock, USDA information systems and client devices will conceal information previously visible on display screens by displaying publicly viewable images that will not contain CUI. The publicly viewable images may be static or dynamic, such as screen savers, blank screens, photographic images, or display non-sensitive device information such as the current time and remaining battery life.
- e. Agencies may not exempt session lock requirements for all accounts on an information system or service. When there is a mission need to exempt specific accounts from implementing session lock requirement, agencies will document those accounts and rationale in the SSP.

## 15. SESSION TERMINATION

Session termination ends all processes associated with a user's logical session except for those processes that the user specifically created to continue after terminating the session. Logical sessions are terminable without terminating the network session.

The following requirements apply to USDA information systems with a moderate- or high-impact categorization:

- a. Agencies will specify in the SSP the conditions and trigger events that result in the termination of a user's session;
- b. USDA information systems will automatically terminate and require re-authentication to re-establish a user-initiated logical session:
  - (1) After 30 minutes of inactivity; and
  - (2) After the occurrence of agency-specified conditions or trigger events.
- c. Agencies will not waive session termination requirements systemwide. If there is a mission need to exempt one or more system accounts from implementing session termination, the agency will request a waiver for the specific accounts or devices.

## 16. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

- a. Agencies will identify actions that users may perform on information systems without requiring user identification and authentication and document them in SSPs. Actions that may not require identification and authentication include accessing publicly available USDA websites, answering incoming phone calls, replying to text messages on USDA-issued mobile devices, and receiving fax transmissions on networked fax machines or all-in-one printers.
- b. Agencies will identify and document in the SSP any action that may exist that are exempt from the identification and authentication requirements under certain circumstances, such as in an emergency.

## 17. REMOTE ACCESS

Remote access encompasses any connection to a USDA information system or component originating from outside of a USDA owned and operated network infrastructure, such as accesses for telework and mobile work.

- a. Access to USDA information systems using Government furnished laptops and mobile devices while on domestic travel will meet the requirements in DR 3580-004, or while on international travel will meet the requirements in DR 3580-005.

- b. Agencies will identify the approved remote access methods for users to access agency information systems.
- c. Agencies will establish usage restrictions, configuration and connection requirements, and implementation guidance for the permitted remote access methods and document them in the SSP.
- d. Remote access requirements will not apply to users accessing USDA public web servers and other publicly accessible systems.
- e. Agencies will ensure that USDA information systems that allow remote access include automated monitoring capabilities to detect and control access attempts by auditing remote access connection activities on a variety of devices.
- f. Agencies will ensure that remote access methods:
  - (1) Employ NIST [FIPS PUB 140-2](#), *Security Requirements for Cryptographic Modules* certified encryption and mutual authentication;
  - (2) Route all remote access sessions through a limited number of USDA Trusted Internet Connection network-access control points;
  - (3) Permit connections to USDA remote client devices only after verifying the client device has been scanned for malware;
  - (4) Employ a multifactor authentication method identified in Section 7a(2); and
  - (5) Transmit and transfer data via an encrypted VPN in compliance with [DM 3530-005](#), *Encryption Security Standards*.
- g. Agencies will document and set conditions (e.g., VPN, encrypted channel) for the execution of privileged commands and access to security-relevant information via remote access methods.

## 18. WIRELESS ACCESS

- a. Before allowing wireless connections, each wireless technology used to access a USDA information system will:
  - (1) Be authorized by the Mission Area Assistant Chief Information Officer (CIO), or designee;
  - (2) Identify usage restrictions, configuration and connection requirements, and implementation guidance and document them in the SSP; and
  - (3) Only permit wireless access authentication protocols that provide mutual device authentication and protect the confidentiality and integrity of user authentication

credentials by implementing encryption technologies in accordance with DM 3530-005.

- b. Agencies will identify and explicitly authorize users approved to independently configure wireless networking capabilities, such as:
  - (1) Permitting users to configure their USDA client device to connect to home networks and to peripheral devices as indicated in DR 3580-004; and
  - (2) Permitting network administrators to configure USDA wireless access points and wireless settings for USDA backbone servers and devices.
- c. Access enforcement mechanisms will be configured to prevent unauthorized changes to wireless networking capabilities (see DR 3580-004 for additional guidance to allow users some capabilities to manage wireless protocols).
- d. USDA client devices will be configured with the strongest Bluetooth security and encryption modes supported by the device, as discussed in NIST [SP 800-121](#), Revision 2, *Guide to Bluetooth Security*, and have auto-pairing functionality disabled.
- e. USDA client devices will be configured to prohibit connections to multiple networks simultaneously (e.g., disable a laptop's wireless capability when it is connected to a wired network).
- f. USDA information systems that are wireless-capable, categorized as high impact, and located within Government owned or controlled buildings will implement strategies to minimize the unauthorized access to or use of Institute of Electrical and Electronics Engineers ([IEEE](#)) [802.11](#) wireless communications from outside of USDA facilities, by:
  - (1) Calibrating radio antennas to reduce transmission power and signal strength;
  - (2) Employing electromagnetic shielding measures to control wireless emanations; or
  - (3) Using beam-forming antennas.

## 19. ACCESS CONTROL FOR MOBILE DEVICES AND LAPTOPS

The requirements in this section apply to USDA-owned or USDA-controlled client devices issued by agencies. Section 20 provides access requirements for client devices that are not USDA-owned or controlled.

- a. Agencies will:
  - (1) Establish usage restrictions; device identification, integrity, and configuration requirements in accordance with DR 3520-002; authentication and connection requirements; and implementation guidance for each type of laptop and mobile device consistent with DR 3580-004;

- (2) Implement anti-malware software and firewalls in accordance with [DR 3575-002](#), *System and Information Integrity*, including updating anti-malware software and scanning for malware;
  - (3) Scan for misconfigurations and current and missing software updates and patches in accordance with [DR 3530-006](#), *Scanning and Remediation of Configuration and Patch Vulnerabilities*; and
  - (4) Disable unauthorized or unnecessary mobile capabilities, such as wireless and infrared device capabilities.
- b. Agencies will ensure that all Government furnished laptops and mobile devices that connect to USDA information systems employ encryption in accordance with DR 3580-004.

## 20. USE OF EXTERNAL INFORMATION SYSTEMS

External information systems include personally owned devices, such as bring your own device (BYOD). Agencies that allow BYOD will adhere to the requirements in DR 3xxx-xxx, the BYOD policy.

- a. Requirements in this section do not apply to external information systems that access public interfaces to USDA information systems, including publicly accessible USDA websites.
- b. Information systems managed by other Federal Agencies or other governmental organization (e.g., state, local, tribal) will be treated as external information systems when they do not have an established trust relationship (e.g., memorandum of agreement or interconnection security agreement) with USDA.
- c. All non-Government furnished information systems will be treated as external information systems and adhere to the requirements in DR 3580-004, prior to allowing access to USDA information systems.
- d. Agencies will only permit authorized individuals to access an external information system or to process, store, or transmit organization-controlled information when an approved information system connection or processing agreement has been established with the external information system provider.
- e. Agencies will prohibit the connection of USDA-controlled removable media to external information systems.
- f. Additional guidance about removable media can be found in DR 3580-005.

## 21. INFORMATION SHARING

- a. Factors for agencies to consider when developing information sharing procedures include:
  - (1) Ensure personnel involved in the information sharing process are trained on their roles (i.e., for marking, handling, or sharing sensitive information or CUI), as needed;
  - (2) Agency procedures may require qualified personnel to review or approve information prior to being released, or may require a signed memorandum of agreement with an external party prior to sharing the information;

Note: The NARA website, [CUI Registry: Limited Dissemination Controls](#), provides dissemination principles. Other NARA website references in Appendix A provide training about CUI that may be useful in information sharing procedures.

- (3) Agency procedures may also, for example, require information systems to display or print information markings, enforce dual authorization requirements prior to electronically transferring information, or enforce sharing restrictions based on signed agreements.
- b. Agencies with information systems categorized as moderate or high impact will additionally develop and implement procedures to:
    - (1) Facilitate information sharing by enabling authorized users to determine whether requests for access to information they control meet the criteria for granting access to others (i.e., determine whether information with a restriction such as privileged medical, contract sensitive, or classified can be shared with a person internal or external to USDA); and
    - (2) Implement manual processes or automated mechanisms to assist users in making information sharing and collaboration decisions.

## 22. PUBLICLY ACCESSIBLE CONTENT

- a. Agencies will explicitly designate individuals authorized to post information on publicly accessible USDA information systems.
- b. Agencies will develop and implement processes to:
  - (1) Train authorized users to ensure that publicly accessible information does not contain non-public information;
  - (2) Ensure only authorized users post information approved for public release;

- (3) Ensure information intended for public release is reviewed prior to it being posted on a publicly accessible information system;
- (4) Conduct monthly reviews of publicly accessible information systems for non-public information; and
- (5) Remove non-public information from publicly accessible systems when discovered, maintain a log of the information removed, and institute measures to prevent a recurrence.

## 23. ROLES AND RESPONSIBILITIES

### a. The USDA CIO will:

- (1) Ensure that Departmental policy and delegations of authority for access control are developed and implemented in support of this DR; and
- (2) Ensure agencies have adequate resources to carry out access control requirements.

### b. The USDA Chief Information Security Officer (CISO) will:

- (1) Ensure the development and maintenance of Departmental access controls in accordance with this DR;
- (2) Maintain oversight to ensure the Department and agencies develop, maintain, and comply with policies, procedures, and access control techniques; and
- (3) Ensure Mission Area Assistant CIOs, CISOs, and Information Systems Security Program Managers (ISSPM) receive updated Federal and Departmental access control requirements and guidance.

### c. Mission Area Assistant CIOs will:

- (1) Assign responsibilities to support and implement this policy;
- (2) Ensure policies, procedures, guidance, processes, and checklists, as appropriate, are developed;
- (3) Ensure the resources needed to maintain secure local and remote access capability are included in each USDA agency IT budget; and
- (4) Approve the use of wireless technologies, mobile devices, and accessories used to connect with information systems.

### d. CISOs and ISSPMs will:

- (1) Provide guidance and enforce the policies, procedures, processes, and checklists developed to comply with this policy;

- (2) Ensure the access control procedures, processes, and checklists are reviewed and, if necessary, updated;
- (3) Ensure that access controls are reviewed, appropriately tested, and, if necessary, promptly corrected;
- (4) Ensure the security controls to external information systems maintain an acceptable level of risk to information and information systems;
- (5) Ensure access control requirements are documented and submitted to the USDA CISO for inclusion in Departmentwide compliance reporting, as needed;
- (6) Ensure access control standards including methods, technology, devices, configurations, and tools balance risk and business needs;
- (7) Advise system owners about the secure implementation of wireless technologies;
- (8) Ensure that staff involved with controlling access to information and information systems are appropriately trained in accordance with DR 3545-001 and authorized to perform those duties;
- (9) Ensure auditing is enabled and audit records are created for all account and privilege activities; and
- (10) Ensure that privileged users cannot make unauthorized changes to audit settings.

e. System Owners or Account Managers will:

- (1) Ensure the processes to create, maintain, revoke, and verify access controls and privileges implement the security concepts of need-to-know, least privilege, and separation of duties to produce accurate and desired results, and comply with this policy;
- (2) Maintain information for all applicable system accounts, and ensure account deactivation when individuals no longer require access;
- (3) Approve the roles, accounts, groups, and appropriate privileges assigned to each to implement on information systems;
- (4) Coordinate with information stewards to decide who has access to the information system and determine the types of privileges and access rights;
- (5) Approve any accounts exempt from the automatic disabling function;
- (6) Establish criteria for authorizing and reviewing account types, privileges, roles, and account and group memberships;
- (7) Ensure that USDA information systems implement appropriate access control mechanisms, including both discretionary and mandatory access controls;

- (8) Ensure assignment of, or changes to, user access and privileges to information systems are implemented only with approved authorizations;
  - (9) Ensure that privileged accounts are associated with a specific user unless a shared system or service account is required and is specifically authorized;
  - (10) Ensure that users, including information system support staff, are trained before being granted access to the information system, in accordance with DR 3545-001;
  - (11) Ensure users formally agree to abide by the system's rules of behavior and terms of use prior to gaining information system access; and
  - (12) Ensure that staff involved with access controls are appropriately trained and are authorized to manage access.
- f. Information Stewards will:
- (1) Provide input to system owners regarding:
    - (a) The roles that have access to information and their privileges; and
    - (b) The security requirements and controls needed to protect information where it is processed, stored, or transmitted.
  - (2) Establish rules for appropriate use and protection of information in information sharing environments and retain that responsibility even when the information is shared with, or provided to, other organizations.
- g. Managers or Supervisors will:
- (1) Request new, modified, or terminated access to information systems for employees and other USDA personnel; and
  - (2) Apply the security concepts of need-to-know, least privilege, and separation of duties when requesting creation or modification of user account accesses and privileges.
- h. CORs will:
- (1) Maintain an accurate position description for each contract position;
  - (2) Submit, in advance of contractor work or access, the necessary information to initiate or verify the contractor's background investigation, commensurate with the sensitivity described in the position description and the systems and level of access the contractor will require;
  - (3) Request new, modified, or terminated access for contractor personnel to information systems; and

- (4) Apply the security concepts of need-to-know, least privilege, and separation of duties when requesting creation or modification of user account accesses and privileges.
- i. System and Network Administrators will:
    - (1) Implement and maintain access controls in accordance with this policy and any updated guidance from Federal authoritative sources;
    - (2) Monitor the effectiveness of access controls, take corrective action when appropriate, and submit monitoring reports as required;
    - (3) Review system audit records for indications of inappropriate usage and report findings to designated organizational officials, as specified in internal procedures; and
    - (4) Generate and archive documentation upon request or as established in procedures to provide evidence of compliance with this policy.
  - j. Users will:
    - (1) Have and maintain a current, favorably adjudicated background investigation in accordance with Federal requirements prior to gaining access to an information system;
    - (2) Complete annual training for information security awareness and protecting personally identifiable information, per DR 3545-001, and sign the rules of behavior and an acceptable use agreement;
    - (3) Complete annual specialized role-based information security training specific to their roles or duties, if designated as having significant security responsibilities;
    - (4) Review [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, annually;
    - (5) Notify their supervisor if an access control vulnerability or policy violation is discovered or suspected;
    - (6) Report any suspicious or unusual activity to their supervisor as soon as possible; and
    - (7) Conduct remote network access activities securely and in compliance with applicable Departmental and agency policies and procedures.

## 24. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DR 4070-735-001, Section 16, sets forth USDA policies, procedures, and standards on employee responsibilities and conduct regarding the use of computers and

telecommunications equipment. In addition, DR 4070-735-001, Section 21, *Disciplinary or Adverse Action*, states:

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

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

## 25. POLICY EXCEPTIONS

- a. All USDA agencies are required to conform to this policy. If a policy requirement cannot be met as explicitly stated, a waiver may be requested. Note that an approved waiver does not bring the system into compliance with policy. Requests for waivers:
  - (1) Are an acknowledgement of a system's non-compliance with policy and that an acceptable plan to remediate the weakness has been provided and will be implemented; and
  - (2) Must be documented as indicated in [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1.
- b. Policy waiver request memorandum will be addressed to the USDA CISO and submitted to [ISC.Outreach@usda.gov](mailto:ISC.Outreach@usda.gov) for review and decision. Unless otherwise specified, approved policy waivers must be reviewed and renewed every fiscal year.

## 26. INQUIRIES

Address inquiries concerning this DR to Office of the Chief Information Officer (OCIO), Information Security Center (ISC) via email to the [csc@usda.gov](mailto:csc@usda.gov) mailbox.

-END-

## APPENDIX A

### AUTHORITIES AND REFERENCES

*Administrative Personnel*, [Title 5, CFR 731](#), (2018)

*The Atomic Energy Act 1954*, as Amended, [Public Law 114-92](#) (2015)

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

Department of Homeland Security, Homeland Security Presidential Directive 12 ([HSPD-12](#)), *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004

[EO 13467](#), *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information*, June 30, 2008

[EO 13488](#), *Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust*, January 16, 2009

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

[EO 13556](#), *Controlled Unclassified Information*, November 9, 2010

[EO 13764](#), *Amending the Civil Service Rules, Executive Order 13488, and Executive Order 13467 To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters*, January 17, 2017

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

IEEE, Standards Association, [802.11 wireless local area network standards](#)

NARA, [CUI: Additional Tools](#)

NARA, [CUI Registry: Limited Dissemination Controls](#)

NARA, [CUI Training Tools](#)

NARA, [General Records Schedule 3.2: Information Systems Security Records](#), September 2016

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

NIST, [Access Control Policy Testing](#)

NIST, [FIPS PUB 140-2](#), *Security Requirements for Cryptographic Modules*, (includes change notices as of December 3, 2002), May 25, 2001

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

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

NIST, [National Checklist Program Repository](#)

NIST, National Institute of Standards and Technology Interagency Report [\(NISTIR\) 6192](#), *A Revised Model For Role-Based Access Control*, July 9, 1998

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

NIST, [NISTIR 7316](#), *Assessment of Access Control Systems*, September 2006

NIST, [NISTIR 7874](#), *Guidelines for Access Control System Evaluation Metrics*, September 2012

NIST, [NISTIR 7966](#), *Security of Interactive and Automated Access Management Using Secure Shell (SSH)*, October 2015

NIST, [NISTIR 7987, Revision 1](#), *Policy Machine: Features, Architecture, and Specification*, October 2015

NIST, [NISTIR 8112](#), *Attribute Metadata, A Proposed Schema for Evaluating Federated Attributes*, January 2018

NIST, [SP 800-46, Revision 2](#), *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*, July 29, 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 800-57](#), *Recommendation for Key Management – Part 2: Best Practices for Key Management Organization*, August 2005

NIST, [SP 800-70, Revision 4](#), *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*, February 2018

NIST, [SP 800-100](#), *Information Security Handbook: A Guide for Managers*, March 2007

NIST [SP 800-121, Revision 2](#), *Guide to Bluetooth Security*, May 2017

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

NIST, [SP 800-162](#), *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, February 2019

NIST, [SP 800-178](#), *A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications: Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)*, October 2016

NIST, [SP 800-192](#), *Verification and Test Methods for Access Control Policies/Models*, June 2017

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

OPM, [Investigation Process Details](#)

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

OMB, [M-11-11](#), *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011

OMB, [M-14-03](#), *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013

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

OMB, Memorandum [M-05-24](#), *Implementation of Homeland Security Presidential Directive (HSPD) 12 - Policy for a Common Identification Standard for Federal Employees and Contractors*, August 5, 2005

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 2016

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

USDA, [DM 4620-002](#), *Common Identification Standard for U.S. Department of Agriculture Employees and Contractors*, January 14, 2009

USDA, DR 3xxx-xxx, *Bring Your Own Device*, forthcoming

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

USDA, DR 35xx-xxx, *Identification and Authentication*, forthcoming

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

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

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

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

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

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

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

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

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

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

USDA, [DR 4620-002](#), *Common Identification Standard for U.S. Department of Agriculture*, September 29, 2014

USDA, [DR 4720-001](#), *USDA Onboarding Requirements*, June 3, 2011

## APPENDIX B

### DEFINITIONS

Access Control. The process of granting or denying specific requests: (1) for obtaining and using information and related information processing services; and (2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances). (Source: CNSS, CNSSI 4009)

Access Control Policies. Specify how to control accesses between subjects (e.g., individuals or software acting on behalf of individuals) and objects (e.g., information, information systems, and components of information systems) in information systems.

Authentication. Verifying the identity of a user, process, or device as a prerequisite to allowing access to resources in an information system. (Source: NIST, SP 800-53, Revision 4)

Authorization. Access privileges granted to a user, program, or process or the act of granting those privileges. (Source: CNSS, CNSSI 4009)

Automated Mechanism. A software function with characteristics that results in increasing the efficiency, chance of a desired outcome, or reducing the risk of failure or manipulation, in an entire, or a part of, a process.

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)

#### 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 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."

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)

Discovery. Discovery is the process of identifying, locating, securing, and producing evidence, including testimony, things, information, and materials for utilization in the legal process. The term is also used to describe the process of reviewing all materials which may be potentially relevant to the issues at hand and/or which may need to be disclosed to other

parties, and of evaluating evidence to prove or disprove facts, theories, or allegations. There are several formalized methods of conducting discovery, the most common of which are interrogatories, requests for production of documents and depositions. (Source: USDA, DR 3090-001)

Discretionary Access Control. Leaves a certain amount of access control to the discretion of the object's owner, or anyone else who is authorized to control the object's access. The owner can determine who should have access rights to an object and what those rights should be. (Source: NIST, SP 800-192)

Dual Authorization. See Dual Control.

Dual Control. A process that uses two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. No single entity is able to access or use the materials, e.g., cryptographic keys. (Source: NIST, SP 800-57)

Electronic Discovery (ediscovery). The process of collecting, preparing, reviewing, and producing Electronically Stored Information (ESI) in the context of the legal process. See Discovery. (Source: USDA, DR 3090-001)

External Information System (or Component). An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness. (Source: NIST, SP 800-53, Revision 4)

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

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

Group. An object in an authentication system where a collection of accounts is associated that shares common access attributes or privileges based on job function. For example, personnel that maintain an application have their accounts associated with an administrator group and are granted the attributes and privileges assigned to the group.

High-Impact System. An information system in which at least one security objective (e.g., confidentiality, integrity, or availability) is assigned a FIPS PUB 199 potential impact value of high. (Source: NIST, FIPS PUB 200)

Impact. The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system. (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. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. (Source: NIST, SP 800-53, Revision 4)

Information System Component. A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products. (Source: NIST, SP 800-128)

Least Privilege. The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. (Source: CNSS, CNSSI 4009)

Low-Impact System. An information system in which all three security objectives (e.g., confidentiality, integrity, and availability) are assigned a FIPS PUB 199 potential impact value of low. (Source: NIST, FIPS PUB 200)

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

Malware. See Malicious Code. (Source: NIST, SP 800-53, Revision 4)

Mandatory Access Control. Access control policy decisions are made by a central authority, not by the individual owner of an object. Users cannot change access rights. An example of mandatory access control occurs in military security, where an individual data owner does not decide who has a top-secret clearance, nor can the owner change the classification of an object from top-secret to secret. (Source: NIST, SP 800-192)

Media. Physical devices or writing surfaces including but not limited to magnetic tapes, optical disks, magnetic disks, Large Scale Integration memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. (Source: NIST, NISTIR 7298, Revision 2)

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)

Moderate-Impact System. An information system in which at least one security objective (e.g., confidentiality, integrity, or availability) is assigned a FIPS PUB 199 potential impact value of moderate, and no security objective is assigned a FIPS PUB 199 impact value of high. (Source: NIST, FIPS PUB 200)

Multifactor Authentication. Authentication using two or more factors to achieve authentication. Factors include: (1) something you know (e.g. password or personal identification number (PIN)); (2) something you have (e.g., cryptographic identification device, token); or (3) something you are (e.g., biometric). (Source: NIST, NISTIR 7298, Revision 2)

Need-to-Know. A method of isolating information resources based on a user's need to have access to that resource in order to perform their job but no more. The terms need-to-know and least privilege express the same idea. Need-to-know is generally applied to people, while least privilege is generally applied to processes. (Source: NIST, NISTIR 7298, Revision 2)

Network Access. Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). (Source: NIST, SP 800-53, Revision 4)

Non-USDA personnel. Personnel that are not members of "USDA personnel" but use or maintain information systems for, or on behalf of, USDA. For example, state or local government or citizens that are users of USDA information systems; administrators of cloud systems that are operated for, or on behalf of, USDA.

Object. Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object by a subject implies access to the information it contains. Also, see Subject. (Source: NIST, SP 800-53, Revision 4)

Personal Computer (PC). A desktop or laptop computer. (Source: NIST, SP 800-46, Revision 2)

Privileged Account. An information system account with authorizations of a privileged user. (Source: NIST, SP 800-53, Revision 4)

Privileged Command. A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. (Source: NIST, SP 800-53, Revision 4)

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)

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: NIST, SP 800-46, Revision 2)

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 Client Device. A device in the two categories of client devices (PCs and mobile devices) defined by NIST used to access USDA information systems remotely. The term is used in place of NIST's "telework client device."

Role. A mechanism that represents a job function used to determine which group, or groups, (see "Group," above) will be assigned to the user. In role-based access control information systems the role conveys attributes (e.g., a collection of permission or privileges) to the user assigned that role, but in this DR the term "group" is used as the conveyance of attributes or privileges.

Security Controls. The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (Source: NIST, FIPS PUB 199)

Security Functions. The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based. (Source: NIST, SP 800-53, Revision 4)

Security Technical Implementation Guide (STIG). Based on Department of Defense (DoD) policy and security controls. Implementation guide geared to a specific product and version. Contains all requirements that have been flagged as applicable for the product that has been selected on a DoD baseline. (Source: CNSS, CNSSI 4009)

Separation of Duties. A security principle that divides critical functions among different staff members to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud. (Source: NIST, SP 800-57)

Service Account. A mechanism that is created by the installation of an operating system or an application, or is created by an administrator, to enable operating system or application components to execute. This category of account should not be interactive as its purpose or intended use is for software components, not users.

Session Lock. A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system level but may be at the application level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workdays. (Source: NIST, SP 800-53, Revision 4, see control AC-11 - supplemental guidance)

Shared Account. A single mechanism that provides common access rights and privileges to multiple users of an information system. A shared account is also referred to as a “group account.” Users that need the shared account to gain access attributes and privileges are provided with the shared account password. In general, a shared account does not uniquely identify users of the account. Usually, other security practices are employed to uniquely identify personnel that are logged into the shared account. Shared accounts include guest/anonymous accounts, emergency program staff accounts, and some types of administrative accounts.

Subject. Generally, an individual, process, or device causing information to flow among objects or change to the system state. See Object. (Source: NIST, SP 800-53, Revision 4)

System Account. A mechanism that cannot, or should not, be deleted. This category of account usually comes from the vendor, with the system or application may be called a “built-in” or “default account.” This type of account is interactive but should have any default or vendor-created password changed to a strong password and then be disabled or set so that it is not used except in an emergency.

System Security Plan (SSP). Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements. (Source: NIST, NISTIR 7298, Revision 2)

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: USDA, DR 4080-811-002)

Telework Client Device. A PC or mobile device used by a teleworker for performing telework.

United States Government Configuration Baseline (USGCB). The USGCB provides security configuration baselines for information technology products widely deployed across the Federal Agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal Governmentwide initiative that provides guidance to Agencies on what should be done to improve and maintain effective configuration settings focusing primarily on security. (Source: NIST, NISTIR 7298, Revision 2)

USDA Employee. A Federal civil servant employed by, detailed or assigned to, USDA, including members of the Armed Forces.

USDA Personnel. USDA employees, contractors, affiliates, interns, fellows, and volunteers who work for, or on behalf of, USDA, and whose work is overseen by USDA employees.

User. Individual, or (system) process acting on behalf of an individual, authorized to access an information system. (Source: NIST, SP 800-53, Revision 4)

User Account. A mechanism that provides a single individual with access rights and privileges to an information system. Upon authenticating to a user account, a person (the user) is uniquely identified to an information system and is granted the access rights and privileges assigned to that specific account.

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)

Wireless Technologies. Wireless protocols used by client devices (e.g., IEEE 802.11, cellular), and those used by computer accessory devices such as keyboards, speakers, trackballs, and mice (e.g., Bluetooth, infrared, radio frequency).

## APPENDIX C

### ACRONYMS AND ABBREVIATIONS

|            |   |
|------------|---|
| BYOD       | Bring Your Own Device   |
| CFR        | Code of Federal Regulations                                       |
| CIO        | Chief Information Officer   |
| CISO       | Chief Information Security Officer                                |
| CNSS       | Committee on National Security Systems                            |
| CNSSI      | Committee on National Security Systems Instruction                |
| COR        | Contracting Officer's Representative                              |
| CUI        | Controlled Unclassified Information                               |
| DISA       | Defense Information Systems Agency                                |
| DM         | Departmental Manual   |
| DoD        | Department of Defense   |
| DR         | Departmental Regulation   |
| ediscovery | Electronic Discovery  |
| EO         | Executive Order   |
| ESI        | Electronically Stored Information                                 |
| FIPS PUB   | Federal Information Processing Standards Publication              |
| FISMA      | Federal Information Security Modernization Act                    |
| HSPD       | Homeland Security Presidential Directive                          |
| IEEE       | Institute of Electrical and Electronics Engineers                 |
| ISC        | Information Security Center                                       |
| ISSPM      | Information Systems Security Program Manager                      |
| IT         | Information Technology  |
| NARA       | National Archives and Records Administration                      |
| NIST       | National Institute of Standards and Technology                    |
| NISTIR     | National Institute of Standards and Technology Interagency Report |
| OCIO       | Office of the Chief Information Officer                           |
| OGC        | Office of the General Counsel                                     |
| OHS        | Office of Homeland Security                                       |
| OMB        | Office of Management and Budget                                   |
| OPM        | Office of Personnel Management                                    |
| PC         | Personal Computer   |
| PIN        | Personal Identification Number                                    |
| PIV        | Personal Identity Verification                                    |
| SOP        | Standard Operating Procedure                                      |
| SP         | Special Publication   |
| SSP        | System Security Plan  |
| STIG       | Security Technical Implementation Guide                           |
| U.S.C.     | United States Code  |
| USDA       | United States Department of Agriculture                           |
| USGCB      | United States Government Configuration Baseline                   |
| VPN        | Virtual Private Network   |

## APPENDIX D

### SYSTEM USE NOTIFICATION BANNER EXAMPLE

Notice! Authorized Use Only.

You are accessing a U.S. Government information system, which includes: (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices and storage media attached to this network or to a computer on this network. This information system is provided for U.S. Government authorized use only.

Unauthorized or inappropriate use of this system is prohibited and may result in disciplinary action, as well as civil and criminal penalties.

By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this information system. At any time, the Government may, for any lawful Government purpose monitor, record, search, and seize any communication or data transiting or stored on this information system.

Any communications or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose.

Your consent is final and irrevocable. You may not rely on any statements or informal policies purporting to provide you with any expectation of privacy regarding communications on this system, whether oral or written, by your supervisor or any other official, except USDA's Chief Information Officer.

Clicking OK affirms your legal consent and agreement to the above notice.

## APPENDIX E

### DISCUSSION OF LOGICAL ACCESS CONTROL TERMS

This section organizes and explains some logical access control terms used in this DR and defined in Appendix B.

- a. “Access control policies” specify how to control accesses between subjects (e.g., individuals or software acting on behalf of individuals) and objects (e.g., information, information systems, and components of information systems) in information systems;

- b. Account Terms:

Four terms are used in this DR to describe accounts. Section 6a(2) of this DR requires these account types, when used in an information system, be identified in the system security plan (SSP) along with the conditions for their use.

- (1) A “user account” is a mechanism that provides a single individual with access rights and privileges to an information system. Upon authenticating to a user account, a person (the user) is uniquely identified to an information system and is granted the access rights and privileges assigned to that specific account;
- (2) A “shared account” (often referred to as a “group account”) is a single mechanism that provides common access rights and privileges to multiple users of an information system. Users that need the shared account to gain access attributes and privileges are provided with the shared account password. In general, a shared account does not uniquely identify users of the account. Usually, other security practices are employed to uniquely identify personnel that are logged into the shared account;

Shared accounts include guest/anonymous accounts, emergency program staff accounts, and some types of administrative accounts;

- (3) A “system account” is a mechanism that cannot, or should not, be deleted. This category of account usually comes from the vendor, with the system or application may be called a “built-in” or “default account.” This type of account is interactive but should have any default or vendor-created password changed to a strong password and then be disabled or set so that it is not used except in an emergency;
- (4) A “service account” is a mechanism that is created by the installation of an operating system or an application, or is created by an administrator, to enable operating system or application components to execute. This category of account should not be interactive as its purpose or intended use is for software components, not users.

- c. Role-Based Access Terms:

The terms “role” and “group” describe how administrators efficiently manage accounts and attributes by joining each user account to a mechanism, rather than assigning attributes to each user, shared, system, or service account.

NISTIR 7298, Revision 2, defines “role” as “a group attribute that ties membership to function. When an entity assumes a role, the entity is given certain rights that belong to that role. When the entity leaves the role, those rights are removed. The rights given are consistent with the functionality that the entity needs to perform the expected tasks.”

Note that in NIST’s definition, a role is an attribute of a group that ties group membership to a function. This DR provides more detailed definitions for the way privileges are associated with job functions.

In this DR:

- (1) A “role” is a mechanism that represents a job function used to determine which group, or groups, will be assigned to the user. In some information systems a role may convey attributes or privileges, but in this DR a “group” conveys attributes or privileges; and
- (2) A “group” refers to an object in an authentication system where a collection of accounts is associated that shares common access attributes or privileges based on job function. For example, personnel that maintain an application have their accounts associated with an administrator group and are granted the attributes and privileges assigned to the group.

Both NIST’s and this DR’s definition of role indicate that a user’s job function is the driver in determining which privileges are assigned to a user. The user’s role indicates which groups, and therefore which privileges, are assigned to the user after authentication.

d. User Terms:

- (1) “User” is an individual, or (system) process acting on behalf of an individual, authorized to access an information system. (Source: NIST SP 800-53, Revision 4); and
- (2) “Privileged User” is 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).

A user becomes a privileged user when assigned to a role that is permitted to perform security-relevant functions, and by logging into an account, or when assigned to a group (after authentication) that permits execution of a privileged command.

e. The following terms are derived from the definitions above:

- (1) An information system “user account” (e.g., standard, non-privileged account) permits authorized access to an information system and prevents a user (e.g., standard user) from performing security-relevant functions.
- (2) An information system “user group” permits authorized access to an information system and prevents a user (e.g., standard user) from performing security-relevant functions.
- (3) A “privileged account” is an information system account with approved authorizations of a privileged user.

In other words, an information system privileged account permits an authorized user to perform security-relevant functions.

A privileged account may be either a privileged network account or a privileged local system account.

- (4) An information system “privileged group” permits an authorized user to perform security-relevant functions.