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

DEPARTMENTAL REGULATION	NUMBER: DR 3545-003
SUBJECT: Suitability Requirements Permitting Personnel Access to Information Systems	DATE: September 16, 2021
OPI: Office of the Chief Information Officer, Information Security Center	EXPIRATION DATE: September 16, 2026

1. PURPOSE

a. This Departmental Regulation (DR):

(1) Is the United States Department of Agriculture (USDA) policy for assessing the suitability of personnel to access USDA information resources;

(2) Sets the criteria for personnel to gain and maintain access to USDA information and information systems; and

(3) Defines the standards by which personnel establish and maintain a level of trust (e.g., suitability, fitness, and credentialing).

b. This DR serves as the foundation for Mission Areas, agencies, and staff offices to develop and implement their own personnel security procedures.

c. This DR meets the requirements of:

(1) *The Federal Information Security Modernization Act of 2014* (FISMA), 44 United States Code (U.S.C.) § 3551, *et seq.*;

(2) The Office of Management and Budget (OMB), Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* Memorandum M-16-17;

(3) OMB Circular A-130, *Managing Information as a Strategic Resource*;

(4) The National Institutes of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*; and

(5) The personnel security family of controls in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

d. The USDA:

(1) Complies with Federal requirements to assess suitability and fitness of USDA personnel to access USDA information and information systems;

(2) Confirms its management commitment to comply with the authorities governing USDA personnel security for access to information and information systems;

(3) Supports personnel security activities for protecting USDA information and information systems; and

(4) Continually manages risks to those systems.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This DR is effective when published and will remain in effect until superseded or expired.

b. All Mission Areas, agencies, and staff offices will align their procedures with this policy within 6 months of the publication date.

c. This DR is a supplement to DR 4720-001, *USDA Onboarding Requirements*.

d. Other related directives include:

(1) Departmental Manual (DM) 4620-002, *Common Identification Standard for U.S. Department of Agriculture Employees and Contractors*;

(2) DR 3505-003, *Access Control for Information and Information Systems*;

(3) DR 3505-005, *Cybersecurity Incident Management*;

(4) DR 3640-001, *Identity, Credential, and Access Management*;

(5) DR 4600-001, *USDA Personnel Security Clearance Program*; and

(6) DR 4620-002, *Common Identification Standard for U.S. Department of Agriculture*.

3. SCOPE

a. This policy applies to:

(1) All Mission Areas, agencies, staff offices, and all USDA personnel;

(2) Information, information systems, and cloud-based services used or operated by, for, or on behalf of USDA. These include interconnections between or among these information systems or services; and

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

(a) Facilities owned or operated by USDA; or

(b) Facilities owned or operated on behalf of USDA by a contractor, subcontractor, or other organization.

b. This policy guides senior executives and managers to provide the resources necessary to establish:

(1) Eligibility for employment;

(2) The identity, suitability, and fitness of personnel to perform work for, or on behalf of, the USDA; and

(3) Procedures to issue USDA credentials for access to Federal buildings and USDA information systems.

c. Nothing in this policy alters the requirements for protecting national security systems or information. This includes those identified in FISMA and the Committee on National Security Systems (CNSS) policies and standards. It also includes intelligence community policies, directives, and instructions.

4. BACKGROUND

USDA personnel hold roles with a variety of privileges and access. Personnel are vital in protecting USDA information and information systems. Personnel must act responsibly with their privileges and access. As such, USDA personnel must also guard against malicious use or exploitation of legitimate access, per DR 4600-003, *USDA Defensive Counterintelligence and Insider Threat Programs*.

The unauthorized disclosure, access, use, disruption, modification, destruction, or the loss of control of sensitive information can erode public trust in USDA. It can also cause adverse financial impacts to USDA.

Security techniques establish suitable levels of trust for USDA personnel. These techniques include background investigations, assigning a risk designation to each position, completing access agreements, managing privileges, and terminating access in a timely manner. All of these can also minimize risks to USDA information and information systems.

5. POLICY

a. Each Mission Area, agency, and staff office will:

(1) Develop and implement procedures that address personnel suitability standards described in this DR for granting access to USDA information and information systems;

(2) Review the procedures annually;

(3) Update them to reflect changes in policy;

(4) Disseminate them to stakeholders;

(5) Assign position risk designations and sensitivity levels for all Government and contractor positions;

(6) Review the position designations at least annually; and

(7) Update them as needed using the Office of Personnel Management (OPM) *Position Designation Automated Tool* (PDT).

b. The procedures will:

(1) Require USDA personnel to obtain and maintain favorable background investigations, based on the position sensitivity levels and risk designations;

(2) Ensure that USDA personnel receive favorable background investigations or Federal Bureau of Investigation (FBI) fingerprint checks (per DM 4620-002) that meet or exceed the requirements for the intended positions;

(3) Ensure USDA personnel submit their background investigation requests to Defense Counterintelligence and Security Agency (DCSA);

Note: See the DCSA website *Requesting Personnel Investigations via e-QIP*, for additional information.

(4) Allow for the reciprocal use of current and favorable background investigations from other Federal agencies, as long as they meet or exceed the requirements for the intended positions.

(5) Allow managers or Contracting Officer's Representatives (COR) to request approval for personnel to begin performing some duties, per DM 4620-002:

(a) After they submit their background investigation forms to the DCSA; and

(b) The FBI fingerprint check does not return derogatory information.

(6) Ensure managers follow the guidance in DR 3440-001, *USDA Classified National Security Information Program Regulation* and DR 4600-001 if the position requires access to classified information.

c. The procedures for granting access to USDA information or systems will include processes to:

(1) Update background investigations when USDA personnel change positions (e.g., relocation or promotion) or the position requirements change (e.g., additional access to more sensitive or classified materials), per DR 3440-001, DR 4600-001, and DR 3440-003, *Controlled Unclassified Information (CUI) Program*; and

(2) Add, remove, or change physical or logical access, as needed, when USDA personnel change duties or locations within USDA.

d. The procedures will require all personnel to sign access agreements that:

(1) Define their personal responsibilities;

(2) Inform them of appropriate use, conduct, actions, and behavior permitted on, or when using, Departmental information systems; and

(3) Serve to acknowledge that they understand these conditions.

e. Mission Areas, agencies, and staff offices will:

(1) Develop and document access agreements based on information type and sensitivity level for each category of information or information system;

(2) Review the agreements at least annually and update them as needed;

(3) Ensure that USDA personnel:

(a) Acknowledge their understanding of the access agreement, by handwritten or digital signature, prior to being granted access to information and information systems; and

(b) Review and acknowledge the access agreement annually, or when the agreement is updated.

(4) Describe acceptable and improper uses of information systems that include:

(a) A provision that USDA personnel are permitted access to, and use of, USDA systems to carry out their USDA responsibilities; and

(b) A clear explanation that limited personal use of USDA information systems is allowed but does not extend to improper use of the systems.

f. Mission Areas, agencies, and staff offices will develop procedures and implement measures to prevent, detect, track, and report improper use.

g. The following activities are prohibited and amount to improper use of USDA information systems:

(1) Intentionally changing or attempting to change information security controls that protect against unauthorized access;

(2) Downloading unauthorized software, such as peer-to-peer sharing apps and illegal or copyrighted materials;

(3) Distributing illegally-obtained files or software;

(4) Permitting or enabling unauthorized access to any USDA information system for any purpose;

(5) Engaging in inappropriate activities or those likely to offend fellow employees or the public. This includes:

(a) Accessing sexually explicit materials; and

(b) Using hate speech or remarks to ridicule others based on age, race, creed, religion, skin color, sex, physical or mental handicap, or national origin.

(6) Accessing or attempting to access any USDA information system for unauthorized purposes, such as:

(a) Invasion of privacy; and

(b) Obtaining information that the user is not authorized to access, use, disclose, modify, or destroy.

h. The procedures for personnel departing USDA (permanently or temporarily) will include the follow:

(1) Retrieve all USDA-issued property, assets, and systems;

(2) Transfer any sensitive information to an authorized individual;

(3) Disable all physical and logical access;

(4) Archive and disable information system accounts, per DR 3505-003; and

(5) Follow guidance in DR 4600-002, *Procedures for the Denial or Revocation of Access to National Security Information*, when involving access to classified information or systems.

i. Mission Areas, agencies, and staff offices will ensure that contracts and other agreements with external providers include requirements to:

(1) Ensure that personnel security processes, such as on-boarding, off-boarding, and reassignments, meet or exceed USDA personnel security requirements in this policy and in DR 4020-250-002, *Position Management and Vacancy Control*;

(2) Notify USDA Contracting Officers and CORs of personnel changes to contracted services (e.g., adding or removing personnel to contract support staff). This enables timely granting, modifying, or suspension of access rights and privileges, and the return of Government-furnished equipment; and

(3) Provide their documented personnel security processes, as evidence of compliance.

6. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) will:

(1) Ensure Mission Areas, agencies, and staff offices develop procedures to implement this policy;

(2) Ensure personnel suitability, fitness, and credentialing goals for access to USDA information and information systems meet Federal requirements and standards; and

(3) Coordinate, as needed, with the:

(a) Director of the Office of Homeland Security (OHS);

(b) Chief Security Director of the Office of Safety, Security, and Protection (OSSP); and

(c) Mission Area Assistant CIOs to ensure procedures have been developed.

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

(1) Lead the Departmental information security program;

(2) Develop and implement the USDA information security program plan;

(3) Ensure the program plan includes suitability standards defined in this DR and the Personnel Security control family in NIST SP 800-53, Revision 5;

(4) Update the program and program plans, as needed, to meet changes to requirements; and

(5) Ensure compliance with the information security program across the USDA.

c. The Chief Security Director of the OSSP will:

(1) Ensure the protection of the Department's physical facilities;

(2) Provide physical security assessments and review them on a recurring basis;

(3) Manage and maintain a comprehensive physical security program at USDA facilities in the National Capital Region (NCR); and

(4) Manage the credentialing processes and goals for USDA personnel, ensuring the Department meets Federal requirements and standards.

d. The Director of the OHS will:

(1) Guide personnel security staff (PSS) and provide information updates, as needed;

(2) Coordinate with PSS to ensure background investigations are current for all USDA personnel serving in positions designated as moderate or high risk;

(3) Coordinate with Mission Area Assistant CIOs and Mission Area Human Resource Directors (MAHRD) on matters of USDA personnel security;

(4) Serve as the Senior Agency Official (SAO) for USDA personnel security, unless formally designated to another official; and

(5) When serving as the SAO for USDA personnel security, provide guidance to mitigate actual or suspected insider threats.

e. The Director of the Office of Human Resource Management (OHRM) will:

(1) Coordinate with the Director of the OHS and the Chief Security Director of the OSSP to ensure consistency between processes;

(2) Ensure OHRM processes for personnel actions (e.g., on-boarding, reassignments, and off-boarding) integrate with OHS and OSSP processes, and;

(3) Implement automated and non-automated mechanisms for personnel termination notification.

f. The MAHRDs, or similar role if an MAHRD is not assigned, will:

(1) Ensure that Mission Area personnel procedures are consistent with Departmental requirements;

(2) Coordinate with Information Systems Security Managers (ISSM) and PSS to ensure that Mission Area personnel procedures include OHS and OSSP guidance; and

(3) Coordinate the completion of all suitability tasks, defined in this DR, between subordinate agencies and staff offices, the OSSP, and the OHS Personnel and Document Security Division (PDSD).

g. PSS will:

(1) Develop, implement, and update relevant training materials;

(2) Provide input to USDA personnel security processes; and

(3) Coordinate with and provide guidance to Mission Area Assistant CIOs and MAHRD on matters of USDA personnel security.

h. Mission Area Assistant CIOs will:

(1) Ensure that Mission Area Assistant CISOs and ISSMs maintain consistent processes and procedures between their agencies, and staff offices;

(2) Ensure the processes and procedures:

(a) Meet Federal and Departmental requirements; and

(b) Enforce personnel security standards, as noted in this DR, for access to information resources.

i. Mission Area Assistant CISOs and ISSMs will:

(1) Coordinate with their MAHRD to assign position sensitivity levels and risk designations;

(2) Coordinate with CORs to ensure compliance with this policy and that contracts include specific penalties for non-compliance;

(3) Ensure all USDA personnel and external providers comply with this policy and other applicable Federal and USDA guidance for on-boarding, off-boarding, and USDA personnel reassignments; and

(4) Coordinate with their MAHRD, as needed, to maintain accurate and current records for personnel actions related to accessing facilities, information, and information systems.

j. CORs will:

(1) Review the requirements and guidance from OHRM, OHS, OSSP, and this DR, to ensure consistency in contract language;

(2) Ensure contract language requires contractors to have corporate processes that establish employment suitability and fitness;

(3) Obtain documents from contractors, when warranted, as proof that:

(a) Their personnel security processes and guidance on ethical behavior are fully implemented; and

(b) They are consistent with USDA requirements.

(4) Coordinate on-boarding and off-boarding of contractor personnel with the OHS, the OSSP, and other stakeholder offices when necessary.

k. System Owners will:

(1) Implement a process to add, remove, or change accesses and privileges;

(2) Approve system access requests only after the requester completes all required actions; and

(3) Support investigations of possible violations of the Rules of Behavior (RoB) or misuse of USDA information systems.

l. Managers and Supervisors will:

(1) Coordinate with the appropriate ISSM, Mission Area Assistant CISO, or MAHRD when defining or changing position risk and sensitivity designations;

(2) Ensure all USDA personnel under their direct supervision:

(a) Complete the annual security awareness and privacy training, per DR 3545-001, *Information Security Awareness and Training Policy* (including forthcoming update) and DR 3515-002, *Privacy Policy and Compliance for Personally Identifiable Information (PII)*;

(b) Acknowledge they understand the behavior and conduct standards;

(c) Sign all access agreements; and

(d) Maintain required background investigations.

(3) Guide USDA personnel about actions that may:

(a) Violate acceptable use;

(b) Constitute a misuse of USDA resources; or

(c) Be contrary to the standards of ethical conduct.

(4) Assist personnel with reporting suspected violations, adhering to guidance in DR 3505-005;

(5) Seek guidance from higher-level managers or other competent authorities in matters of ethical conduct or acceptable use; and

(6) Coordinate with OHS, OHRM, OSSP, and contract managers, when needed, for disciplinary or personnel termination actions.

m. USDA Personnel will:

(1) Complete the annual security awareness and privacy training, per DR 3545-001 and DR 3515-002;

(2) Acknowledge they understand the RoB by signing an access agreement form prior to accessing any USDA information systems;

(3) Adhere to the RoB and ethical conduct;

(4) Use caution before taking any action that may be a violation of the RoB, acceptable use, or may run contrary to ethical conduct; and

(5) Report any suspected or perceived violations of the RoB to a manager.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DR 4070-735-001, *Employee Responsibilities and Conduct*, Section 16, sets forth the USDA policy for employee responsibilities and standards of conduct. This includes the use of computers and telecommunications equipment (also see DR 3300-001, *Telecommunications & Internet Services and Use*, section 2b and DR 3300-026, *Planning and Managing Wireless Technologies*, section 5g for additional guidance). In addition, DR 4070-735-001,Section 21, *Disciplinary or Adverse Action*, states:

a. Any violation of the responsibilities or standards contained in this DR may be cause for disciplinary or adverse action; and

b. Any disciplinary or adverse action will be consistent with the applicable laws and regulations.

These include the *Standards of Ethical Conduct for Federal Employees of the Executive Branch.* 5 Code of Federal Regulations (CFR) Part 2635, as well as other OPM or OMB regulations.

8. POLICY EXCEPTIONS

a. All Mission Areas, agencies, and staff offices will conform to this policy. They may request a waiver if they cannot meet a policy requirement as explicitly stated. Note that an approved waiver does not constitute compliance with policy. Requests for waivers:

(1) Acknowledge the non-compliance with policy;

(2) Commit to implement an acceptable plan to remediate the weakness; and

(3) Document the plan as indicated in DR 3565-003, *Plan of Action and Milestones Policy*.

b. Address policy waiver requests to the USDA CISO. Submit the requests for review and decision to ISC.Outreach@usda.gov. Unless otherwise specified, review and renew approved policy waivers each fiscal year.

9. INQUIRIES

Send any questions or concerns about this DR to the Office of the Chief Information Officer (OCIO), Information Security Center (ISC) via email to cscc@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
COR	Contracting Officer's Representative
CSRC	Computer Security Resource Center
CUI	Controlled Unclassified Information
DCSA	Defense Counterintelligence and Security Agency
DM	Departmental Manual
DR	Departmental Regulation
E.O.	Executive Order
FBI	Federal Bureau of Investigation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
ISC	Information Security Center
ISSM	Information Systems Security Manager
MAHRD	Mission Area Human Resources Director
NCR	National Capital Region
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OHRM	Office of Human Resource Management
OHS	Office of Homeland Security
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OSSP	Office of Safety, Security, and Protection
PDSD	Personnel and Document Security Division
PDT	Position Designation Automated Tool
PSS	Personnel Security Staff
RoB	Rules of Behavior
SAO	Senior Agency Official
SOP	Standard Operating Procedure
SP	Special Publication
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

External information system service provider. A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; or supply chain exchanges. (Source: NIST, Computer Security Resource Center (CSRC), *Glossary*, Retrieved August 13, 2019)

Improper usage. Any incident resulting from violation of an organization's acceptable usage policies by an authorized user. (Source: NIST, SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, in the *Executive Summary*)

Information security. The protection of information and systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide confidentiality, integrity, and availability. (Source: NIST, CSRC, *Glossary*, Retrieved August 13, 2019)

Information system. A discrete set of information resources organized for collecting, processing, maintaining, using, sharing, disseminating, or disposing of information. (Source: 44 U.S.C. § 3502, *Definitions*)

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 excluding display media) onto which information is recorded, stored, or printed within an information system. (Source: NIST, CSRC, *Glossary*, Retrieved August 13, 2019)

Organization. An entity of any size, complexity, or positioning within an organizational structure (e.g., Federal agencies, private enterprises, academic institutions, state, local, or tribal governments, or as appropriate, any of their operational elements). (Source: NIST, CSRC, *Glossary*, Retrieved August 13, 2019)

Reciprocity. Reciprocity, as it applies in background investigations, is the practice of accepting background investigations, suitability decisions and security decisions conducted by other authorized Federal agencies. Consistency created by national background investigation standards assists in avoiding duplication of work by allowing one agency to reciprocally accept a background investigation and favorable decision from another agency. See 5 CFR Part 731, *Suitability*; and Executive Order (E.O.) 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* for exceptions and details. (Source: NIST, CSRC, *Glossary*, Retrieved August 13, 2019)

Risk. A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (a) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (b) the likelihood of occurrence. (Source: OMB Circular A-130)

USDA employee. Refers to a Federal civil servant employed by, detailed or assigned to, USDA, including members of the Armed Forces. (Source: 5 U.S.C § 2105, *Employee*; E.O. 12968, *Access to Classified Information*)

USDA personnel. Encompasses USDA employees, contractors, partners, affiliates, interns, fellows, and volunteers who work for, or on behalf of, USDA, and whose work is overseen by USDA employees. (Source: DR 3505-003)

APPENDIX C

AUTHORITIES AND REFERENCES

DCSA, *Requesting Personnel Investigations via e-QIP*, Website

Definitions, 44 U.S.C. § 3502

Designation of public trust positions and investigative requirements, 5 CFR § 731.106

Employee, 5 U.S.C § 2105

E.O. 12968, *Access to Classified Information*, August 2, 1995

E.O. 13526, *Classified National Security Information*, December 29, 2009

E.O. 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

NIST, CSRC, *Glossary* website

NIST, FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006

NIST, SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018

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

NIST, SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012

Office of Government Ethics, *Standards of Ethical Conduct for Federal Employees of the Executive Branch*, 5 CFR Part 2635, *et seq.*

OMB, Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016

OMB, Memorandum M-16-17, *OMB Circular No. A-123, Management's Responsibility for Enterprise Risk Management and Internal Control*, July 15, 2016

OPM, *Position Designation Automated Tool* website

Suitability, 5 CFR Part 731

USDA, DM 3440-001, *USDA Classified National Security Information Program Manual*, June 9, 2016

USDA, DM 3505-005, *Cybersecurity Incident Management Procedures*, November 30, 2018

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

USDA, DR 3300-001, *Telecommunications & Internet Services and Use*, March 18, 2016

USDA, DR 3300-026, *Planning and Managing Wireless Technologies*. January 23, 2020

USDA, DR 3440-001, *USDA Classified National Security Information Program Regulation*, June 9, 2016

USDA, DR 3440-003, *Controlled Unclassified Information (CUI) Program*, September 13, 2021

USDA, DR 3505-003, *Access Control for Information and Information Systems*, July 17, 2019

USDA, DR 3505-005, *Cybersecurity Incident Management*, November 30, 2018

USDA, DR 3515-002, *Privacy Policy and Compliance for Personally Identifiable Information (PII)*, October 30, 2020

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 3640-001, *Identity, Credential, and Access Management*, June 8, 2021

USDA, DR 4020-250-002, *Position Management and Vacancy Control*, October 18, 2010

USDA, DR 4070-735-001, *Employee Responsibilities and Conduct*, October 4, 2007

USDA, DR 4600-001, *USDA Personnel Security Clearance Program*, July 2, 2013

USDA, DR 4600-002, *Procedures for the Denial or Revocation of Access to National Security Information*, September 13, 2013

USDA, DR 4600-003, *USDA Defensive Counterintelligence and Insider Threat Programs*, July 12, 2021

USDA, DR 4620-002, *Common Identification Standard for U.S. Department of Agriculture*, June 24, 2021

USDA, DR 4720-001, *USDA Onboarding Requirements*, June 3, 2011