

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

DEPARTMENTAL REGULATION	NUMBER: DR 3515-002
SUBJECT: Privacy Policy and Compliance for Personally Identifiable Information (PII)	DATE: October 30, 2020
OPI: Office of the Chief Information Officer	EXPIRATION DATE: October 30, 2025

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

1. PURPOSE

- a. This Departmental Regulation (DR) establishes the United States Department of Agriculture (USDA) privacy policy, provides the impetus and foundations for the Privacy Program, and guides the development of associated processes and procedures.
- b. It is USDA policy to comply with Federal requirements to establish, implement, and support a Departmental Privacy Program and associated program plans to continually manage risks to privacy data, Personally Identifiable Information (PII), and USDA's information resources.
- c. This directive establishes USDA policy and compliance with the *E-Government Act of 2002*, as amended, [44 United States Code \(U.S.C.\) § 3501](#); the *Confidential Information Protection and Statistical Efficiency Act of 2002*, [44 U.S.C. § 3501](#); the *Privacy Act of 1974*, [5 U.S.C. § 552](#) (as amended); the *Clinger-Cohen Act of 1996*, [40 U.S.C. 11101 et seq.](#); and Office of Management and Budget (OMB) policies and guidance.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This policy supersedes Departmental Manual (DM) 3515-000, *Privacy Requirements*, dated February 17, 2005.
- b. This policy is effective immediately and remains in effect until superseded or expired.
- c. All USDA Mission Areas, agencies, and staff offices will align their policies and procedures with this DR within 6 months of the publication date.
- d. The term “USDA personnel” means USDA employees, contractors, affiliates, interns, fellows, and volunteers who work for, on behalf of, USDA, and whose work is overseen by USDA employees.

3. SCOPE

This policy applies to all USDA Mission Areas, agencies, and staff offices and USDA personnel working for, or on behalf of, USDA regarding the collection, use, maintenance, disclosure, deletion, destruction, or dissemination of PII, in transit and at rest, for official purposes and regarding any other activity that impacts the privacy of individuals, as determined by the USDA Senior Agency Official for Privacy (SAOP).

4. BACKGROUND

The legal rights of individuals are guaranteed and must be protected regarding the collection, use, maintenance, disclosure, deletion, destruction, or dissemination of PII in compliance with Federal laws, regulations, and policies. This DR provides direction and guidance to Mission Areas, agencies, and staff offices for implementing those requirements.

5. POLICY

- a. The Department will comply with OMB memoranda [M-01-05](#), *Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy*; [M-03-22](#), *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*; [M-05-08](#), *Designation of Senior Agency Officials for Privacy*; [M-11-02](#), *Sharing Data While Protecting Privacy*; and [M-16-24](#), *Role and Designation of Senior Agency Officials for Privacy*.
- b. The Department will comply with OMB Circulars [A-108](#), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, and [A-130](#), *Managing Information as a Strategic Resource*, Appendix II: *Responsibilities for Managing Personally Identifiable Information*, which include the *Fair Information Practice Principles*, as guidelines for USDA’s privacy policy.

- c. The Department will comply with OMB specific guidance on Privacy management and control requirements, to include the safeguarding of PII, in accordance with OMB memoranda.
- d. USDA Mission Areas, agencies, and staff offices will coordinate with the Chief Privacy Officer (CPO), or designee, when developing and implementing privacy policy and procedures to ensure they are consistent with Federal laws, regulations, guidance, and Departmental policy.
- e. USDA Mission Areas, agencies, and staff offices will ensure all personnel have received privacy training, and provide support to Departmental leadership on privacy-related matters, data gathering, reporting requirements, and privacy-related investigations and incident reporting.
- f. USDA Mission Areas, agencies, and staff offices , through their Privacy Officers, Privacy Act Officers, Privacy Analysts, and other Privacy Points of Contact (PPOC), will coordinate with the CPO, or designee, to ensure that their processes and procedures follow USDA privacy policy and standards; thereby enhancing the overall consistency of privacy protections across USDA.
- g. All privacy policies and associated procedures and controls will be reviewed annually and updated, if necessary, within 1 year of the issuance of changes in Federal law, regulations, and OMB and National Institute of Standards and Technology (NIST) guidance.
- h. USDA Mission Areas, agencies, and staff offices may develop privacy policies, processes, and procedures that meet, or exceed corresponding Departmental policy requirements if needed, to further enhance Departmental privacy policy. However, those policies, processes, and procedures will neither contradict, nor be less stringent than, Departmental policy requirements.

6. ROLES AND RESPONSIBILITIES

- a. The Secretary of Agriculture will:
 - (1) Ensure that all PII and information systems within which PII is stored, processed, or transits, are protected in compliance with all Federal requirements;
 - (2) Ensure that privacy and PII management processes are integrated into USDA's strategic, operational, budgetary, and acquisition planning processes;
 - (3) Be accountable for managing the cybersecurity risks to PII maintained by USDA, in both electronic and hard-copy format;
 - (4) Designate a senior official at the Deputy Assistant Secretary or equivalent level who serves in a central leadership position, that has the necessary skills, knowledge,

and expertise to lead, direct, and carry out the privacy-related functions described in law and OMB policies, as the SAOP; and

(5) Delegate the necessary authority to the SAOP to carry out all assigned duties.

b. The USDA CIO will:

(1) Serve as the USDA SAOP;

(2) Serve as the Department's official point of contact on all matters related to privacy in the Federal Government;

(3) Govern the USDA Privacy Program;

(4) Review and approve USDA's privacy policy and procedures to ensure they are comprehensive, current, and compliant with applicable privacy laws and Federal guidance;

(5) Be responsible for the overall management of the Department's Privacy Program portfolio, to include budget management;

(6) Chair the Data Integrity Board (DIB);

(7) Coordinate with the USDA Chief Information Security Officer (CISO) to provide guidance regarding information technology and technology-related programs to develop and implement policies and procedures to safeguard PII used or maintained by the Department, in accordance with Federal law and policy;

(8) Coordinate with the Director, Office of Contracting and Procurement, serving as the Senior Procurement Executive, to ensure that contract provisions related to assisting with a breach and breach notifications are uniform and consistently included in agency contracts;

(9) Coordinate with the Assistant Secretary for Civil Rights on privacy issues related to civil rights and civil liberties arising from Departmental activities, such as collections, privacy violations, PII security incidents, development of policy, procedures, and contract language, as required;

(10) Ensure all USDA personnel receive appropriate training and education regarding their privacy protection responsibilities;

(11) Ensure Departmental preparedness for and responding to an incident or breach, to include development, implementation, and testing of a breach response plan;

(12) Ensure Departmental, Mission Area, agency, and staff office incident management and breach response plans and procedures are developed, disseminated, fully implemented, and periodically tested (with test results and artifacts documented, analyzed to identify weaknesses, and retained for audit and investigation purposes);

- (13) Represent USDA at the Federal Privacy Council;
- (14) Ensure Departmental development and evaluation of legislative, regulatory, and related policies address privacy issues and involve privacy collaborations, as needed;
- (15) Review, approve, and maintain a list of all Departmental information systems that process, store, collect PII, or facilitate the transfer of PII between information systems;
- (16) Ensure that Federal statutory and regulatory reporting requirements, OMB guidelines, USDA Departmental directives, and other applicable guidance have been met;
- (17) Submit applicable reports as required on the USDA Privacy Program; and
- (18) Designate and appoint the USDA CPO.

c. The USDA CPO will:

- (1) Establish, coordinate implementation, and ensure compliance with USDA Departmental privacy policy and supplemental guidance. The CPO establishes the privacy policy, subject to review and approval by the CISO, and SAOP;
- (2) Evaluate Departmental directives, rulemakings, technologies, policies, procedures, guidelines, programs, projects, and systems (including pilot activities), whether proposed or operational, for potential privacy impacts and advise USDA leadership and Mission Area, agency, and staff office heads on implementing corresponding privacy protections, providing approval as appropriate;
- (3) Coordinate with Mission Area, agency, and staff office heads, Privacy Officers, Privacy Act Officers, Privacy Analysts, and other Mission Area, agency, and staff office heads PPOCs to ensure that the Department follows USDA privacy policies, OMB memoranda, applicable privacy laws, and Federal Governmentwide privacy policies regarding protecting PII;
- (4) Chair the USDA Privacy Council meetings and ensure adherence to the *Privacy Council Charter*, forthcoming;
- (5) Serve as the DIB Secretary and ensure adherence to *DIB Charter*, forthcoming;
- (6) Process privacy complaints from organizations and individuals regarding Departmental activities and ensuring redress is provided, as appropriate;
- (7) Review privacy incidents or matters relating to possible violations of privacy arising from the administration of any Department program or operations;

- (8) Ensure that the Department's privacy reports are transmitted to OMB and Congress, as applicable;
 - (9) Provide technical assistance to system and program managers, as needed, in the development of privacy documentation; and
 - (10) Coordinate with the USDA CIO, the USDA CISO, and the Director of the Office of Homeland Security (OHS) to provide guidance regarding information technology and technology-related programs to develop and implement policies and procedures to safeguard PII used or maintained by the Department in accordance with Federal law and policy.
- d. The USDA CISO will:
- (1) Review and approve Departmental directives and waivers related to privacy protection administration;
 - (2) Ensure the annual Information Security Awareness and Training incorporates provisions for protecting privacy and privacy information;
 - (3) Ensure privacy documentation reviews for Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA) are incorporated into the security assessment and authorization process;
 - (4) Collaborate with CPO on PII practices involving information system security to include, but not limited to, PII breaches, system reviews to include privacy and security controls, and compliance; and
 - (5) Formulate budget allocations and provide staffing resources for privacy personnel and the CPO, supporting the Departmental Privacy Office.
- e. The Director, Office of Contracting and Procurement, will:
- (1) Coordinate with the SAOP to ensure that contract provisions related to assisting with a breach and breach notifications are uniform and consistently included in agency contracts.
- f. The Assistant Secretary for Civil Rights will:
- (1) Coordinate with the SAOP on privacy issues related to civil rights and civil liberties arising from Departmental activities, such as collections, privacy violations, PII security incidents, development of policy, procedures, and contract language, as required.
- g. Mission Area Assistant CIOs will:
- (1) Ensure all USDA personnel protect PII, regardless of format or media type;

- (2) Ensure all USDA personnel are familiar with and adhere to USDA privacy directives;
 - (3) Ensure completion of the required privacy compliance documentation in a timely manner;
 - (4) Ensure all information necessary to meet the Department's reporting requirements regarding privacy-related USDA activities is provided to the CPO in a timely manner;
 - (5) Assist the CPO in reviewing USDA activities related to privacy protections, ensuring they are fully integrated into operations, that privacy incidents and privacy complaints are being addressed, and that an avenue for redress is provided, as appropriate;
 - (6) Provide financial resources and other support for their respective Mission Area, agency, and staff office component Privacy Officers, Privacy Act Officers, Privacy Analysts, and other PPOCs to ensure effective implementation of all aspects of USDA privacy policy;
 - (7) Ensure that Mission Area, agency, and staff office contracts for activities that involve PII or otherwise impact the privacy of individuals include appropriate language requiring that Departmental contractors follow USDA privacy policy and this directive; and
 - (8) Ensure Mission Area, agency, and staff office personnel are informed and aware of the Departmental breach notification procedures as outlined in the *USDA Incident Response Plan (IRP)*, forthcoming.
- h. Mission Area, Agency, and Staff Office System and Program Managers will:
- (1) Be knowledgeable and follow the Departmental breach notification procedures as outlined in the *USDA Incident Response Plan (IRP)*, forthcoming;
 - (2) Prepare and submit privacy documentation for approval to the USDA CPO, including any new or altered data to be collected such as changes to PTA and PIA documents;
 - (3) Prepare and submit System of Records Notice (SORN) and supplementary documentation to the USDA CPO for review;
 - (4) Actively reduce the collection of Social Security Numbers or Taxpayer Identification Numbers unless stipulated by law and done in support of conducting USDA business;
 - (5) Ensure compliance with other USDA privacy policies and the [*Privacy Policy Statement*](#); and

- (6) Prepare and submit Computer Matching Agreement (CMA) and supplementary documentation to the USDA CPO for review, in accordance with [DR 3450-001](#), *Computer Matching Program Involving Personally Identifiable Information*.
- i. Privacy Officers, Privacy Act Officers, Privacy Analysts, and other PPOCs will:
 - (1) Maintain documentation regarding system compliance with information privacy laws, Federal regulations, and Departmental directives;
 - (2) Develop, review, and revise system PTA, PIA, SORN, CMAs, Cost Benefit Analyses, and Memoranda of Understanding as applicable to the Departmental Privacy Program for compliance with Federal regulations and applicable laws and guidance;
 - (3) Review all systems annually to ensure system modifications or revisions involving PII are reflected in the current version of the CMA, SORN, and PIA documents;
 - (4) Complete the annual USDA *Protecting Personally Identifiable Information* training course in AgLearn or a vendor-provided course that has been approved by the CPO; and
 - (5) Ensure that Mission Areas, agencies, and staff offices review and update their system or application privacy documentation each fiscal year.
 - j. All USDA Personnel will:
 - (1) Inform individuals from whom they collect information as to why the information is needed, how it will be used, and the reasons it may be disclosed;
 - (2) Take PII training or approved alternative to ensure PII awareness;
 - (3) Ensure that information about individuals is used only for the stated reasons, unless they receive the individual's consent to disclose the information;
 - (4) Ensure that information about individuals is accurate, relevant, and up-to-date;
 - (5) Maintain appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of PII; and
 - (6) Comply with the policies outlined in this directive to safeguard PII information from unauthorized disclosure and immediately report damaged, lost, or stolen USDA PII data to the Department's security incident response team as defined in the USDA *Incident Response Plan (IRP)*, forthcoming.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

Under the *Privacy Act of 1974*, a person can be prosecuted for asking for or taking information under false pretenses. Knowingly and willingly giving someone else's PII to

anyone who is not entitled to it is also a violation. Failure to comply with the *Privacy Act of 1974* can result in a misdemeanor criminal charge, as well as a fine of up to \$5,000 for each offense.

- a. [DM 3300-026](#), *Planning and Managing Wireless Technologies*, Sections 5f, 5g, and 5h, set forth USDA's policies and standards on employee responsibilities and conduct relative to the use of wireless technologies.
- b. [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16, sets forth the USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment, with further delineation provided in [DR 3300-001](#), *Telecommunications & Internet Services and Use*.
- c. DR 4070-735-001, Section 21, *Disciplinary or Adverse Action*, states:
 - (1) A violation of any of the responsibilities and conduct standards contained in the above directive may be cause for disciplinary or adverse action; and
 - (2) Disciplinary or adverse action will be affected in accordance with applicable law and regulations.
- d. [Department Personnel Manual](#), Chapter 751, *Discipline*, Appendix A, *USDA Guide for Disciplinary Penalties*, sets forth penalties for the unauthorized disclosure or use of (or failure to safeguard) information protected by the *Privacy Act of 1974* or other official, sensitive, or confidential information, may be cause for disciplinary action from letter of reprimand to removal.

8. POLICY EXCEPTIONS

All USDA personnel are required to conform to this policy.

- a. All Mission Areas, agencies, and staff offices are required to conform to this policy. There is no waiver from compliance with the provisions of the *Privacy Act of 1974*, as amended. However, if a specific policy requirement, not affiliated with the provisions of the *Privacy Act of 1974*, cannot be met as explicitly stated in this DR, a waiver must be requested. Note that an approved waiver does not result in compliance with policy. Requests for waivers:
 - (1) Are an acknowledgement of 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 the standard operating procedure (SOP) issued by the Compliance and Policy Branch, [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1.

- b. Policy waiver request memorandum will be addressed to the USDA CISO and submitted to ISC.Outreach@usda.gov for review and decision. Unless otherwise specified, approved policy waivers must be reviewed and renewed every fiscal year.

9. INQUIRIES

All questions regarding this DR should be directed to the USDA Privacy mailbox at USDAPrivacy@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMA	Computer Matching Agreement
CPO	Chief Privacy Officer
DIB	Data Integrity Board
DG	Departmental Guidebook
DM	Departmental Manual
DR	Departmental Regulation
FIPS PUB	Federal Information Processing Standards Publication
FISMA	Federal Information Security Modernization Act
NIST	National Institute of Standards and Technology
OHS	Office of Homeland Security
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PPOC	Privacy Point of Contact
PTA	Privacy Threshold Analysis
P.L.	Public Law
SAOP	Senior Agency Official for Privacy
SOP	Standard Operating Procedure
SOR	System of Record
SORN	System of Records Notice
SP	Special Publication
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

- a. Breach. The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for other than authorized purpose. (Source: OMB, [M-17-12](#), *Preparing for and Responding to a Breach of Personally Identifiable Information*)
- b. Computer Matching Agreement (CMA). A written agreement that establishes the conditions, safeguards, and procedures under which a Federal organization agrees to disclose data where there is a computerized comparison of two or more automated Systems of Records (SOR). In conjunction with a CMA, an Interagency Agreement is also prepared when the SORs involved in the comparison are the responsibility of another Federal Agency. (Source: Adapted from [Privacy Act of 1974](#))
- c. Computer Matching Program. A procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-Federal records to find individuals who are common to more than one system or set. The procedure includes all of the steps associated with the match, including obtaining the records to be matched, actual use of the computer administrative and investigative action on the hits, and disposition of the personal records maintained in connection with the match. It should be noted that a single matching program may involve several matches among several participants. There are exclusions to matching programs such as matches done to produce aggregate statistical data without any personal identifiers and matches done by an agency using its own records. (Source: *Privacy Act of 1974*)
- d. Data Integrity Board (DIB). Oversees and coordinates various provisions of the *Privacy Act of 1974* as it relates to the Department's participation in matching programs. (Source: *Privacy Act of 1974*)
- e. Incident. An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (Source: [Federal Information Security Modernization Act \(FISMA\) of 2014](#))
- f. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. (Source: Departmental Guidebook ([DG](#)) [0100-002](#), *USDA Departmental Directives Definitions Glossary*)

Interagency Agreement. A written agreement entered into between two Federal agencies, or major organizational units within an agency, which specifies the goods to be furnished or tasks to be accomplished by one agency (the servicing agency) in support of the other (the requesting agency). (Source: DG 0100-002)

- g. Maintain. Includes collect, use, or disseminate. (Source: *Privacy Act of 1974*)
- h. Personally Identifiable Information (PII). Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Source: DG 0100-002)
- i. Redress. Each agency that maintains a system of records shall – upon request by any individual to gain access to his record in the system, permit him upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence; permit the individual to request amendment of a record pertaining to him. (Source: *Privacy Act of 1974*)
- j. System of Records (SOR). A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying piece of information assigned to the individual. (Source: *Privacy Act of 1974*)
- k. System of Records Notice (SORN). Statement providing public notice of the existence and character of a group of records under the control of any agency, from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying piece of information assigned to the individual. (Source: *Privacy Act of 1974*)

APPENDIX C

AUTHORITIES AND REFERENCES

Clinger-Cohen Act of 1996, [40 U.S.C. § 11101 et seq.](#), February 10, 1996

Computer Matching and Privacy Protection Act of 1988, Public Law ([P.L.](#)) [100-503](#), October 18, 1988

Confidential Information Protection and Statistical Efficiency Act of 2002, [44 U.S.C. § 3501](#), December 17, 2002

E-Government Act of 2002, [44 U.S.C. § 3501](#), December 17, 2002

Federal Information Security Modernization Act (FISMA) of 2014, [44 U.S.C. § 3551-3559](#), December 18, 2014

Electronic Freedom of Information Act Amendments of 1996, [5 U.S.C. § 552](#), October 2, 1996

Federal Records Act of 1950, [44 U.S.C. § 3101](#), September 5, 1950,

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

NIST, Federal Information Processing Standards Publication ([FIPS PUB](#)) [197](#), *Advanced Encryption Standard (AES)*, November 26, 2001

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

NIST, [Special Publication \(SP\) 800-53](#), Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, January 22, 2015

NIST, [SP 800-122](#), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 6, 2010

OMB, Circular [A-108](#), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, revised January 4, 2017

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

OMB, Memorandum [M-01-05](#), *Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy*, December 20, 2000

OMB, [M-03-22](#), *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003

OMB, [M-05-08](#), *Designation of Senior Agency Officials for Privacy*, February 11, 2005

OMB, [M-06-16](#), *Protection of Sensitive Agency Information*, June 23, 2006

OMB, [M-11-02](#), *Sharing Data While Protecting Privacy*, November 3, 2010

OMB, [M-16-04](#), *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, October 30, 2015

OMB, [M-16-24](#), *Role and Designation of Senior Agency Officials for Privacy*, September 15, 2016

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

OMB, *Privacy Act Implementation – Guidelines and Responsibilities*, [40 Federal Register 28.948 and 28.952](#), July 9, 1975

Privacy Act of 1974, [5 U.S.C. § 552a](#), as amended, December 31, 1974

USDA, AgLearn *Protecting Personally Identifiable Information* training course

USDA, [CAPE-SOP-003](#), *Plan of Action and Milestones Management Standard Operating Procedure*, Revision 1.1, November 14, 2015

USDA, [DG 0100-002](#), *USDA Departmental Directives Definitions Glossary*, September 26, 2018

USDA, [DM 3300-026](#), *Planning and Managing Wireless Technologies*, January 23, 2020

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

USDA, [DR 3445-001](#), *Media Protection*, October 30, 2019

USDA, [DR 3450-001](#), *Computer Matching Program Involving Personally Identifiable Information*, October 29, 2020

USDA, [DR 3450-002](#), *Freedom of Information Act Implementing Regulations*, February 7, 2003

USDA, [DR 3505-005](#), *Cybersecurity Incident Management*, November 30, 2018

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

USDA, [Department Personnel Manual](#), Chapter 751, Appendix A, *Guide for Disciplinary Penalties*, June 24, 1994

USDA, *DIB Charter*, forthcoming

USDA, [*Freedom of Information Act Service Center*](#) web page

USDA, *Incident Response Plan (IRP)*, forthcoming

USDA, *Privacy Council Charter*, forthcoming

USDA, [*Privacy Policy Statement*](#) web page