

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

DEPARTMENTAL REGULATION	NUMBER: DR 3450-001
SUBJECT: Computer Matching Program Involving Personally Identifiable Information	DATE: October 29, 2020
OPI: Office of the Chief Information Officer, Privacy Office	EXPIRATION DATE: October 29, 2025

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

1. PURPOSE

This Departmental Regulation (DR) establishes policy and defines roles and responsibilities for conducting United States Department of Agriculture’s (USDA) Computer Matching Programs (CMPs). This DR also addresses the use of computerized comparisons of two or more automated information systems for establishing and verifying Federal benefit program eligibility or recouping payments, delinquent debts, or overpayments owed to Government Agencies from a Federal benefit program.

2. SPECIAL INSTRUCTIONS/CANCELLATIONS

- a. This DR supersedes DR 3450-001, *Computer Matching Projects Involving Individual Privacy Data*, dated April 17, 1984.
- b. This policy is effective immediately and remains in effect until it is superseded or expires.

- c. All Mission Areas, agencies, and staff offices will align their policies and procedures with this policy within 6 months of the publication date.
- d. The terms “regulation” and “policy” may be used interchangeably.
- e. The *Computer Matching and Privacy Protection Act of 1988*, [Public Law \(P.L.\) 100-503](#), will be commonly referred to in this document as the *Computer Matching Act*.

3. SCOPE

This DR applies to all:

- a. USDA Mission Areas, agencies, staff offices, field offices, and program offices;
- b. USDA employees, contractors, interns, partners, volunteers, and affiliates working for, or on behalf of, USDA;
- c. Automated information systems or services (including cloud-based services) used or operated by, for, or on behalf of USDA, including interconnections between or among these systems or services; and
- d. Facilities from which these systems or services operate whether owned or operated by USDA or owned or operated on behalf of USDA by a contractor, subcontractor, or other organization.

4. BACKGROUND

- a. The USDA is committed to preserving and enhancing privacy protections for all individuals, promoting transparency of USDA operations, and serving as a leader in the Federal privacy community. The CMP uses a Computer Matching Agreement (CMA) to fulfill this commitment. A CMA is 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 system of records (SOR).
- b. The *Computer Matching Act* amended the *Privacy Act of 1974*, [5 United States Code \(U.S.C.\) Section 552a](#), and establishes procedural safeguards affecting Agencies’ use of *Privacy Act* SOR while using certain types of CMPs. The *Computer Matching Act* regulates the use of computer matching by Federal Agencies involving personally identifiable records maintained in a SOR subject to the *Privacy Act*. The *Computer Matching Act* requires Agencies to have written agreements in place specifying the terms under which matches are to be conducted and by adding certain protections for individuals applying for and receiving Federal benefits. The *Computer Matching Act* applies to the computerized comparison of two or more automated SORs (or Federal personnel or payroll SORs) between Federal Agencies or between a Federal Agency and

a non-Federal Agency. The *Computer Matching Act* covers two kinds of matching programs:

- (1) Matching that involves establishing or verifying eligibility or compliance with laws and regulations by applicants for recipients and beneficiaries with respect to, cash, in-kind assistance or payments under Federal benefit programs; or recouping payments or delinquent debts under such Federal benefit programs; and
 - (2) Program matches using records from Federal personnel or payroll SOR relating to Federal personnel management.
- c. USDA's CMA procedures are defined in the [USDA OCIO's Information Security Center \(ISC\), Computer Matching Agreement: Standard Operating Procedure](#).
 - d. The *Improper Payments Elimination and Recovery Improvement Act of 2012* (IPERIA), [P.L. 112-248](#), was designed to provide guidance to help Federal Agencies protect privacy while improving the oversight of payments to prevent waste, fraud, and abuse in Federal spending. The Do Not Pay (DNP) Initiative introduced by Office of Management and Budget (OMB) Memorandum [M-13-20](#), *Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative*, implements Section 5 of IPERIA. IPERIA establishes standards and procedures that apply to matching programs conducted exclusively for purposes of the DNP Initiative.
 - e. OMB [Circular A-108](#), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, supplements and clarifies existing OMB guidance, including OMB [Circular A-130](#), *Managing Information as a Strategic Resource*, and the *Privacy Act*. Specifically, OMB Circular A-108 Section 8, *Publishing Matching Notices*; Section 9, *Reporting Matching Programs to OMB and Congress*; Appendix V – *Full Notice of Federal Register Matching Notice Template*; and Appendix VI – *Revision Notice of Federal Register Matching Notice Template*, capture the mechanics of the CMP in a condensed version and are also addressed in the USDA OCIO's ISC, *Computer Matching Agreement: Standard Operating Procedure*.

5. POLICY

USDA will:

- a. Comply with the *Computer Matching Act*;
- b. Establish CMPs when conducting matching of two or more personally identifiable information (PII) records or SORs, as a computerized comparison of SORs for establishing or verifying eligibility or recouping payments for a Federal benefit program, or relating to Federal personnel management. Matching entities may be Federal, state, or local government agencies, as well as contractors for such agencies;

- c. Ensure the Department establishes an internal Data Integrity Board (DIB) to oversee and approve use of CMPs and cost benefit analyses (CBA). The DIB should be composed of senior officials designated by the USDA Senior Agency Official for Privacy (SAOP);
- d. Evaluate and determine if CMPs meets DNP Initiative requirements;

Ensure the *Privacy Act* matching program for the DNP Initiative is termed “Do Not Pay matching program” when matching with at least one of these databases:

- (1) Department Health and Human Services Department, Office of the Inspector General, [List of Excluded Individuals/Entities](#);
- (2) Department of Housing and Urban Development Department, [Credit Alert System or Credit Alert Interactive Voice Response System](#);
- (3) Department of the Treasury, [Office of Foreign Assets Control’s Specially Designated National List](#);
- (4) Department of the Treasury, [Treasury Offset Program](#) Debt Check Database;
- (5) General Services Administration, [System for Award Management](#);
- (6) Internal Revenue Service (IRS), [Automatic Revocation of Exemption List](#);
- (7) IRS, [Exempt Organization Select Check](#);
- (8) IRS, [Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N \(e-Postcard\) Database](#);
- (9) Social Security Administration, [Death Master File](#);
- (10) Social Security Administration, Prisoner Data Maintained in the [Prisoner Update Processing System](#); or
- (11) Commercial database, [American InfoSource Deceased Data](#).

Note: Section 5(b)(1)(B) of IPERIA provides that OMB may designate additional databases for inclusion in the DNP Initiative, in consultation with the appropriate Agencies and additional considerations. The DNP matching programs have alternative standards and procedures as provided in M-13-20 and the USDA OCIO ISC, *Computer Matching Agreement: Standard Operating Procedure*.

6. ROLES AND RESPONSIBILITIES

- a. The USDA Chief Information Officer (CIO) will:
 - (1) Serve as the USDA SAOP;

- (2) Provide executive leadership and overall management for the Department's Privacy Program;
 - (3) Allocate resources to implement and operate the Departmental Privacy Program;
 - (4) Review, approve, and implement USDA's CMP policy;
 - (5) Sign transmittal letters for a new or modified matching program.
 - (6) Review, approve, and maintain a list of the systems across the Department that process or collect PII;
 - (7) Ensure that Federal statutory and regulatory requirements, guidelines, Departmental directives, and other applicable guidance are met.
 - (8) Chair the DIB; and
 - (9) Designate the Department's senior agency officials who will comprise the DIB;
- b. The DIB will:
- (1) At a minimum, consist of the USDA SAOP and the Inspector General or their designee. Additional members may include any senior officials designated by the SAOP, to include the USDA Chief Privacy Officer (CPO), who serves as the DIB Secretary.
 - (2) Oversee and coordinate the implementation of the *Privacy Act* as it relates to the Department's participation in matching programs;
 - (3) Review, approve, and maintain all Departmental CMAs;
 - (4) Annually review each ongoing matching program in which the Department has participated during the year to:
 - (a) Ensure that the statutory and regulatory requirements, OMB guidelines, and Departmental policies have been met;
 - (b) Assess the costs and benefits of the matching program; and
 - (c) Determine if the matching program should be continued.
 - (5) Review the Department's record-keeping and disposal policies and practices for matching programs to ensure compliance with applicable record retention requirements delineated in:
 - (a) [DR 3080-001](#), *Records Management*;
 - (b) [DR 3085-001](#), *Vital Records Management Program*;

- (c) [DR 3090-001](#), *Litigation Retention Policy for Documentary Materials including Electronically Stored Information*;
 - (d) [DR 3099-001](#), *Records Management Policy for Departing Employees, Contractors, Volunteers and Political Appointees*; and
 - (e) Those published in the National Archives and Records Administration, [General Records Schedules](#);
- (6) Provide interpretation and guidance to the Department's staff on the requirements for matching programs;
 - (7) Serve as the Department's clearinghouse to:
 - (a) Receive and release information on the accuracy, completeness, and reliability of records used in matching programs;
 - (b) Report CMAs to Congress and OMB; and
 - (c) Submit an annual report on matching activities to the Secretary and to OMB;
 - (8) The DIB may also review and report on any Departmental matching activities that are not defined as matching programs under the *Computer Matching Act*.
- c. The CPO will:
- (1) Serve as the DIB Secretary;
 - (2) Administer activities related to the establishment, alteration, or termination of CMAs;
 - (3) Serve as the contact for privacy policies, procedures, and CMAs;
 - (4) Prepare and draft the CMA overview summary presentation to include in the CMP package;
 - (5) Develop, establish, and ensure compliance with Departmental policies and procedures regarding *Computer Matching Act* administration;
 - (6) Review new CMAs, 12-month extension renewals of existing matching programs, CBA, new or altered matching program notices, and new or altered matching program reports prior to submission to the Department's DIB;
 - (7) Prepare an annual report to the USDA Secretary and OMB on current matching agreements;
 - (8) Ensure the Department's DIB transmits any new or altered matching program reports to OMB and Congress;

- (9) Ensure *Notice of Computer Matching Program* is transmitted to the Federal Register (FR) in accordance with *Computer Matching Act*;
 - (10) Provide technical assistance to system and program managers, as needed, in the development of the documentation required for CMAs; and
 - (11) Establish and maintain a list of CMAs, to include effective dates and expirations.
- d. The USDA Chief Information Security Officer will:
- (1) Review and approve new CMAs, 12-month renewals of existing matching programs, or altered matching program reports prior to submission to the Department's DIB; and
 - (2) Provide the Departmental DIB with an Information Technology (IT) security assessment of the CMA and any associated cybersecurity risks.
- e. Mission Area Assistant CIOs will:
- (1) Ensure all personnel are familiar with, and adhere to, the provisions of the CMA, this computer matching DR, and other applicable Departmental policies and procedures;
 - (2) Ensure that a CMA is submitted by USDA Mission Areas, agencies, staff offices, field offices, and program offices participating in CMP, as defined in the *Computer Matching Act*. At USDA, a CMA is also required for "pilot" program matches. Pilot program matches usually last less than 6 months, using the smallest possible sampling of data, or access to data, deemed necessary to test and validate the efficacy of the program being considered. No adverse actions will be taken against an individual whom PII is being matched, based on the results of a pilot program match including stop payments or awards actions;
 - (3) Ensure all CMPs are submitted to the USDA CPO for DIB approval;
 - (4) Provide the CPO with periodic updates (yearly at a minimum) on agency CMPs. Updates, at a minimum, should include title, the Mission Area, agency, or staff office involved in the computer match, DIB approval, FR CMP announcement, computer match commencement, and computer match expiration date; and
 - (5) Report to OMB and Congress any proposal to establish, re-establish, or modify a CMP that would change the purpose, defined elements, matching entities, or change PII variables per Circular A-108.
- f. Mission Area, Agency, and Staff Office Program Managers and Privacy Officers will:
- (1) Prepare and submit CMAs, and related documentation, including any new or altered Matching Program Notice, when the Department is the requestor;

- (2) Ensure the USDA OCIO ISC, *Computer Matching Agreement: Standard Operating Procedure* is used for packet assembly, for all CMPs including the DNP Initiative. Packet assembly should be developed in accordance with OMB Circular A-108, and provide instructions and examples for creating a CMA, supplemental correspondence, process flow, review by the DIB, and notification of Congress;
- (3) Ensure a CBA accompanies the CMA and is reviewed by the DIB. The USDA OCIO ISC, *Computer Matching Agreement: Standard Operating Procedure* has been developed by the USDA CPO for all USDA entities to use. The CBA is foundational and can be refined and expanded in its use;
- (4) Ensure all CMP packets are assembled in accordance with the USDA OCIO ISC, *Computer Matching Agreement: Standard Operating Procedure*, and include:
 - (a) A System of Records Notice (SORN) for the originating systems, where applicable, and identify if a new SORN needs to be developed where a new collection of records is not covered;
 - (b) The current Privacy Impact Assessment (PIA) for applicable originating systems;
 - (c) The current and valid Authorization to Operate (ATO) per [DR 3540-003](#), *USDA Security Assessment and Authorization Policy*, for the originating and participating systems;
 - (d) The current Interconnection Security Agreement (ISA) and any applicable Memorandums of Understanding (MOU);
 - (e) A presentation with overview of the computer matching for the DIB drafted by the USDA Departmental CPO;
 - (f) A Security Design Plan to illustrate the computer matching; and
 - (g) Transmittal letters signed by the SAOP and include a narrative statement and supporting documentation including the proposed matching notice per OMB Circular A-108.
- (5) When applicable, prepare the 12-month extension renewal of an existing CMP, and any required Interagency Transfer of Funds forms per the USDA OCIO ISC, *Computer Matching Agreement: Standard Operating Procedure*;
- (6) Submit draft and final CMAs for review and approval to the Departmental CPO prior to submitting via the Department's executive correspondence management system;
- (7) Ensure CMPs are approved by the DIB and formally vetted via the system;

- (8) Ensure CMAs are posted in the FR for the required comment period prior to the commencement of any matching agreement; and
- (9) Ensure CMAs are available on USDA's web page.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

- a. Under the *Privacy Act*, 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* can result in a misdemeanor criminal charge, as well as a fine of up to \$5,000 for each offense.
- b. [DR 4070-735-001](#), *Employee Responsibilities and Conduct*, Section 16 sets forth USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of computers and telecommunications equipment. DR 4070-735-001, Section 21, 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 shall be effected in accordance with applicable law and regulations.

Such disciplinary or adverse action will be in accordance with applicable law and regulations such Office of Personnel Management and OMB regulations, and the United States Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*, [5 Code of Federal Regulations Part 2635](#).

8. POLICY EXCEPTIONS

Privacy Act provisions cannot be waived. Therefore, exceptions to this policy will not be granted.

9. INQUIRIES

Inquiries about this DR should be directed to the USDA CPO at USDAPrivacy@usda.gov.

-END-

APPENDIX A

ACRONYMS AND ABBREVIATIONS

ATO	Authorization to Operate
CBA	Cost Benefit Analysis
CIO	Chief Information Officer
CMA	Computer Matching Agreement
CMP	Computer Matching Program
CPO	Chief Privacy Officer
DIB	Data Integrity Board
DNP	Do Not Pay
DR	Departmental Regulation
FR	Federal Register
IPERIA	Improper Payments Elimination and Recovery Improvement Act of 2012
IRS	Internal Revenue Service
ISA	Interconnection Security Agreement
ISC	Information Security Center
IT	Information Technology
MOU	Memorandum of Understanding
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
P.L.	Public Law
SAOP	Senior Agency Official for Privacy
SOR	System of Records
SORN	System of Records Notice
U.S.C.	United States Code
USDA	United States Department of Agriculture

APPENDIX B

DEFINITIONS

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 (IAA) is also prepared when the SORs involved in the comparison are the responsibility of another Federal Agency. (Source: *Privacy Act of 1974*, [5 U.S.C. § 552a](#))

Computer Matching Program (CMP). An automated comparison of two or more automated system of records or non-Federal records. The procedure includes all 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. (Source: *Privacy Act of 1974*, [5 U.S.C. § 552a](#))

Data Integrity Board (DIB). The DIB was established under The *Computer Matching and Privacy Protection Act of 1988* which amended the *Privacy Act of 1974*. The DIB purpose is to review, oversee and approve a Federal agency's use of computer matching programs, including the cost benefit analysis. The Act requires that the DIBs be composed of senior officials designated by the head of each agency and Inspector General. (Source: *Privacy Act of 1974*, [5 U.S.C. § 552a](#))

Federal Benefit Program. Any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals. (Source: *Privacy Act of 1974*, [5 U.S.C. § 552a](#))

Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (Source: National Institute of Standards and Technology Information Technology Laboratory, Computer Security Resource Center, [Glossary](#))

Maintaining. The term "maintain" includes maintain, collect, use or disseminate. (Source: *Privacy Act of 1974*, [5 U.S.C. § 552a](#))

Multilateral Computer Matching Agreement. The term multilateral computer matching agreement (multilateral CMA) means a computer matching agreement that involves more than two agencies. The term "multilateral" simply refers to an agreement with multiple parties; it does not refer to an agreement that involves databases outside the United States that are not under the control of a Federal (or non-Federal) Agency. For the purposes of a Do Not Pay matching program involving Treasury's Working System, a multilateral computer matching agreement involves Treasury and more than one payment-issuing agency. (Source: Office of

Management and Budget (OMB), Memorandum [M-13-20](#), *Protecting Privacy while Reducing Improper Payments*)

Personally Identifiable Information (PII). Any information about an individual maintained by an agency, including (a) 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 (b) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Source: General Accountability Office, Report [08-536](#), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008; NIST, Special Publication (SP) [800-122](#), *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*)

Privacy Impact Assessment (PIA). PIA is an analysis of how information is handled: (a) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (b) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (c) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. (Source: *E-Government Act of 2002*, [44 U.S.C. § 3501](#))

System of Record (SOR). A group of any records under the control of any agency from which information is retrieved by the name or by some identifying number, symbol, or other identifying factor assigned to the system. (Source: *Privacy Act of 1974*, [5 U.S.C. § 552a](#))

System of Records Notice (SORN). The term "system of records notice" (SORN) means the notice(s) published by an agency in the Federal Register upon the establishment and/or modification of a system of records describing the existence and character of the system. A SORN identifies the system of records, the purpose(s) of the system, the authority for maintenance of the records, the categories of records maintained in the system, the categories of individuals about whom records are maintained, the routine uses to which the records are subject, and additional details about the system. (Source: OMB, Circular [A-108](#), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*)

APPENDIX C

AUTHORITIES AND REFERENCES

Commercial database, [American InfoSource Deceased Data](#)

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

Department of Health and Human Services Department, Office of the Inspector General, [List of Excluded Individuals/Entities](#)

Department of Housing and Urban Development Department, [Credit Alert System or Credit Alert Interactive Voice Response System](#)

Department of the Treasury, [Office of Foreign Assets Control's Specially Designated National List](#)

Department of the Treasury, [Treasury Offset Program](#) Debt Check Database

E-Government Act 2002, [44 United States Code \(U.S.C.\) § 3501](#), 2002

General Accountability Office, Report [08-536](#), *Privacy: Alternatives Exist for Enhancing Protection of Personally Identifiable Information*, May 2008

General Services Administration, [System for Award Management](#)

Improper Payments Elimination and Recovery Improvement Act of 2012 (IPERIA), [P.L. 112-248](#), January 10, 2013

Internal Revenue Service (IRS), [Automatic Revocation of Exemption List](#)

IRS, [Exempt Organization Select Check](#)

IRS, [Annual Electronic Filing Requirement for Small Exempt Organizations – Form 990-N \(e-Postcard\) Database](#)

National Archives and Records Administration, [General Records Schedules](#)

National Archives and Records Administration and the United States Government Publishing Office, [Federal Register](#)

National Institute of Standards and Technology (NIST), [SP 800-53, Revision 4](#), *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013

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

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

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

Office of Management and Budget (OMB), Circular [A-108](#), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, February 2017, revised

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

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

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

OMB, [M-13-20](#), *Protecting Privacy while Reducing Improper Payments with the Do Not Pay Initiative*, August 16, 2013

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

Social Security Administration, [Death Master File](#)

Social Security Administration, Prisoner Data Maintained in the [Prisoner Update Processing System](#)

United States Department of Agriculture (USDA), *Data Integrity Board Charter*, forthcoming

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

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

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

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

USDA, [DR 3300-001](#), *Telecommunications & Internet Services and Use*, March 8, 2016

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

USDA, DR 3515-xxx, *Privacy Policy and Compliance for Personally Identifiable Information (PII)*, forthcoming

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

USDA, [DR 3650-001](#), *Cloud Computing*, September 30, 2015

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

USDA, Office of the Chief Information Officer, Information Security Center, [Computer Matching Agreement: Standard Operating Procedure](#), September 26, 2019