



Information Security Center (ISC)  
Computer Matching Agreement: Standard Operating Procedure

Version 1.2

9/26/2019

Prepared by the ISC Program Management Office

This document was prepared for authorized distribution only.  
It has not been approved for public release.



## Preface

This document represents [Version 1.2](#) of the [Computer Matching Agreement \(CMA\)](#) Standard Operating Procedure (SOP).

Please refer to the “Document Revision History” for a complete list of changes that have been made to this version prior to its approval.

If you have any comments or questions regarding this document, please contact [USDA Privacy Team](#) at [USDAPrivacy@usda.gov](mailto:USDAPrivacy@usda.gov).



**Document Revision History**

<b>Revision Date</b>	<b>Version</b>	<b>Description</b>	<b>Author(s)</b>
<i>09262019</i>	1.0	<i>OCIO – Information Security Center – Privacy Team</i>	Privacy Team



**Table of Contents**

1.0 Introduction..... 1

2.0 Scope..... 2

3.0 Overview..... 2

4.0 Inputs ..... 4

5.0 Outputs..... 5

6.0 Actors..... 6

7.0 Assumptions..... 6

8.0 Constraints ..... 7

9.0 Procedures..... 7

10.0 Contacts ..... 9

11.0 References..... 9

12.0 Related SOPs ..... 9

13.0 Governing Policies or Guidelines ..... 9

14.0 Acronyms..... 9

16.0 Approvals and Authorization..... 11

  

Table 1. Actors..... 6

Table 2. Contacts ..... 9



## 1.0 Introduction

The United States Department of Agriculture (USDA) is committed to preserving and enhancing privacy protections for all individuals, to promoting transparency of USDA operations, and to serving as a leader in the federal privacy community. It is also the responsibility of the federal government to ensure the protection and safeguarding of Personally Identifiable information in adherence to the [Privacy Act of 1974, 5 United States Code \(U.S.C.\) § 552a, as amended](#).

The [Computer Matching and Privacy Protection Act of 1988](#) (hereafter called Computer Matching Act) amended the Privacy Act by describing the manner in which computer matching involving Federal agencies could be performed. It also added certain protections for individuals applying for and receiving Federal benefits. The Computer Matching Act does not extend Privacy Act coverage to those not originally included or covered by the act. The Computer Matching Act covers two kinds of computer matching programs: (1) Federal benefit programs and (2) records from Federal personnel or payroll systems of records.

For the purpose of these standard operating procedures (SOP), the following definition is copied verbatim from the Computer Matching Act:

- “(8) the term “matching program”—
- (A) means any computerized comparison of—
    - (i) two or more *automated systems* of records or a system of records with non-Federal records for the purpose of—
      - (I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or
      - (II) recouping payments or delinquent debts under such Federal benefit programs, or
    - (ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records...

In support of Government Paperwork Elimination Act (GPEA) [Public Law 105-277](#) and other programs that promote electronic collection. Industry standard practices encourage data sharing and disseminating data while maintaining and providing notification to individual’s personal identifiable information when computer matches are being conducted. GPEA increases the need to publish computer matching agreements (CMAs), with the need to protect individual’s privacy.

E-Government Act of 2002, [Public Law 107-347](#) enhanced the management and promotion of electronic Government services and processes while ensuring adequate protections for privacy of personal information which is a key element of safeguarding computer matching since the matching involves personal identifiable information with other federal or non-federal agencies.



## 2.0 Scope

USDA has outlined and defined its procedures in accordance with the Computer Matching and Privacy Protection Act of 1988. Computer Matching Programs (CMPs) is the overall program that encompasses a CMA and supplemental documents packaged in this guidance and template.

This document should be used in conjunction with Department Regulation ([DR](#)) [3450-001, Computer Matching Programs Involving Individual Privacy Data](#).

## 3.0 Overview

Computer matching is established by creating a CMA. CMAs must be published in the Federal Register *prior to* the implementation of matching. CMAs other than those associated with Do Not Pay (DNP) Initiative have an initial life expectancy of up to 18 months and may be renewed for an additional 12 months. DNP CMAs have an initial life expectancy of up to 36 months and may be renewed for an additional 12 months. Renewals are only honored one time. If the agency needs to continue with a CMA, they must re-establish the agreement, which is synonymous with a new agreement.

In addition to publishing in the Federal Register, CMAs are also required to be posted on the USDA CMA website: <https://www.ocio.usda.gov/about-ocio/policy-e-government-and-fair-information-practices-pef/privacy-office>

USDA must submit a Computer Matching report identifying and detailing current CMAs to the Office of Management and Budget (OMB) annually.

The USDA has developed a CMA template to aid the Information Owner and ensure compliance with applicable privacy requirements in accordance with statutes, federal guidelines and or memorandums, federal policies, and procedures. Agencies shall draft a CMA with enough clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections.

The USDA CMA template provides granular instruction and an outline of the information that needs to be captured in accordance with the Privacy Act of 1974, as amended, [OMB circular A-108](#), [OMB Circular A-130](#), and Chapter 4 of the [Federal Draft Document Handbook](#).

The USDA CMA template and an accompanying Cost Benefit Analysis (CBA), are available as an appendix to this document and are also posted on the Privacy Team's website: <https://www.ocio.usda.gov/about-ocio/policy-e-government-and-fair-information-practices-pef/privacy-office>



All CMA(s) completed after the effective date of this guidance must conform with the guidance contained herein and, in the format, provided in the template. All Sections of the CMA template must be complete and include the following supplemental documentation:

- A CMA Narrative; three transmittal letters (one each to Office of Management and Budget, the Chair of the Senate Committee, and the Chair of the House Committee);
- CBA
- Applicable System of Records Notice (SORN)s;
- Security Design Plan;
- System Security Plan;
- A departmental Privacy Team briefing or presentation;
- Informational memorandum approved by:
  - USDA Chief Information Security Officer (CISO)
  - Addressed to the:
    - USDA Chief Information Officer (CIO),
    - Senior Agency Official for Privacy (SAOP) and
    - The Secretary of Agriculture;
- Documented package review and disposition by the Data Integrity Board.

The structure of the CMA and Computer Matching Congressional and OMB report should be precisely based upon purpose of the match, and must not fall within the realm of the exclusionary clause set forth in [Computer Matching and Privacy Protection Act of 1988](#).

Please do not delete or modify sections of the template. Contact the USDA Privacy Team at [USDAPrivacy@usda.gov](mailto:USDAPrivacy@usda.gov) with any questions or concerns you may have with any information contained in this document or the procedures.



#### 4.0 Inputs

A CMA is required only when all of the three statements below are affirmative:

- a. Does an information system or automated process perform the records match?
- b. Is there at least one entity in the match a Federal agency performing the records match?
- c. Are you comparing two or more Personally Identifiable Information (PII) records or system of records?

A CMA must be prepared if all three responses above are in the affirmative and the efforts or purpose meet at least one of the following conditions:

- a. Creating or checking eligibility or compliance with laws/regulations of applicants or recipients/beneficiaries of a federal program/grant;
- b. Recouping payments, delinquent debts or overpayments owed to government agencies from a federal benefit program; or
- c. Two or more automated Federal personnel or payroll systems of records or a system of Federal Personnel of payroll records with non-federal records.

Once the agency determines that a CMA needs to be implemented, the agency needs to prepare a CMP package consisting of the following and submit it to [USDAPrivacy@usda.gov](mailto:USDAPrivacy@usda.gov):

- Email or routing slip accompanying the package with affiliated system's Authorization to Operate (ATO) expiration date
- Agency's Clearance Sheet, AD 116
- The Computer Matching Agreement
- Cost Benefit Analysis (does not have to be USDA CBA template)
- CMA Narrative Statement
- SORN Notice (Federal Register)
- Transmittal Letters to:
  - OMB Administrator, Office of Information and Regulatory Affairs
  - Chair, Senate Committee on Homeland Security and Governmental Affairs



- Chair, House Committee on Oversight and Government Reform
- System Security Plan(s)(SSP)
- Package review and disposition by the Data Integrity Board

Upon receipt, a member of the departmental Privacy Team will contact the agency to perform a preliminary review and draft some additional key documentation:

- Information memorandum (drafted by the departmental Privacy Team)
- Briefing summarizing the Computer Matching (drafted and developed by the departmental Privacy Team)

The Chief Privacy Officer (CPO) or designee will convene the Data Integrity Board (DIB) to include agency and key members to present the CMA package. The DIB may request additional information prior to the meeting. Upon review of the package, the DIB will provide written disposition of the CMA to the CPO.

Upon approval, the Privacy Office requests that all CMAs and supporting documentation be entered into the Department's Correspondence Control System, currently Enterprise Content Management (ECM) module. The ECM processing code for a CMA is OES097. Agencies are required to use the OES097 processing code in ECM to ensure that the CMA enters into the proper workflow.

Please work with your agency's Correspondence Control Officer for appending documents to ECM. ECM can be accessed using a valid Personal Identity Verification (PIV) card or network login via <https://cms.ess.usda.gov/edm/>. If you're having access problems for ECM, please contact: <https://cms.ess.usda.gov/edm/contact.jsp>

## 5.0 Outputs

The expected output of the process is a completed and signed CMA with supplemental documentation which includes a computer matching program package. An example is shown Appendix A.



### 6.0 Actors

Resources and their respective responsibilities are described in Table 1.

Table 1. Actors

Task	Authorized	Responsible
CMP package: CMA, SORN, CMA Narrative, Transmittal Letters, Privacy Impact Assessment(s) (PIAs), SSP, Security Design Plan, CBA, Informational memoranda, Briefing summary, and clearance sheet	Submitter	Information Owner/ Steward/Privacy Officer or Privacy Point of Contact/Freedom of Information Act Officer, or designee as deemed by agency
CMA package Review	Reviewer and Approval	Data Integrity Board disposition. Attendance includes agency, CPO (serves as Secretary), CISO (serves as facilitator), CIO, and departmental Privacy Team
Review and Approval for CMA package via ECM.	Internal review for stakeholders.	Office of Executive Secretariat (OES) submits in ECM.
Review and Approval for signing documents	Approver	USDA Secretary or designee, SAOP for transmittal letters
Preparation for mailing	Final	Originating agency

### 7.0 Assumptions

Agencies will review their applicable privacy documentation at least annually. Agencies will review their CMA(s) posted on the department’s webpage on a recurring basis and immediately notify Privacy Team of any discrepancies at [USDAPrivacy@usda.gov](mailto:USDAPrivacy@usda.gov).

The Computer Matching report is submitted annually to OMB from the departmental Privacy Team.

The Privacy Act articulates concepts of how the Federal Government should treat individuals and their information. These concepts are known as the Fair Information Practice Principles (FIPPs). The FIPPs impose duties upon Federal agencies regarding the collection, use, dissemination and maintenance of PII. USDA is committed to following the FIPPs listed below:



- Principle of Transparency - USDA must be transparent about what PII it collects, uses, disseminates, and maintains and provide individuals with notice of these applications.
- Principle of Individual Participation - USDA must, to the extent practicable, collect information directly from the individual, as this practice increases the likelihood that the information will be accurate, and give notice to the individual at the time of collection of how the program provides for access, correction, and redress.
- Principle of Purpose Specification - USDA must articulate with specificity the purpose of the program and tie the purpose(s) to the underlying mission of the organization and its enabling authority.
- Principle of Data Minimization - USDA must ensure that any PII collected is directly relevant and necessary to accomplish the specific purpose(s) of the program; this information should only be retained for as long as necessary and relevant to fulfill the specified purposes.
- Principle of Use Limitation - USDA must use and share PII only for the purposes for which USDA collected the information and for which the individual received notice.
- Principle of Data Quality and Integrity - USDA must ensure that PII is accurate, relevant, timely, and complete.
- Principle of Security - USDA must use reasonable security safeguards to protect PII against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
- Principle of Accountability and Auditing - USDA must develop mechanisms to ensure compliance with these principles and with the program's other documentation such as any applicable PIA, SORN, and CMA.

## 8.0 Constraints

The CMA must be published in the Federal Register before any matching can be implemented. Any computer matching done without a current CMA agreement on file is a violation of the Privacy Act of 1974, as amended, and can incur sanctions. The review process for the CMA can be extensive. OMB requires at least 30 calendar days for review, with an additional 30-day extension option.

## 9.0 Procedures

### Step 1 Obtaining the necessary SORN Template

Create the CMA document on your preferred correspondence software application using the CMA template and [Federal Draft Document Handbook](#), Chapter 4 as your guides. The CMA template can be found here: <https://www.usda.gov/privacy>, and select the ***Computer Matching Agreement Template Guidance*** option. Please note that access is generally limited to Privacy



Council members but may be available upon request to the Privacy Team mailbox at [usdaprivacy@usda.gov](mailto:usdaprivacy@usda.gov). Upon access, select and download the latest SORN Template Guidance option.

Step 2 Identify CMA process: New, Renew\* or Re-establishment. Fill out the CMA applicable to purpose—both formats are available in OMB Circular A-108, Appendices V and VI, respectively.

Step 3 Supplemental documentation: Listed above.

Step 4 Submittal to Privacy Team for preparation of Briefing Summary and Informational memorandum.

Step 5 CPO or designee convenes DIB.

Step 6 DIB meets and discusses CMA with stakeholders and departmental Privacy Team. CPO serves as Secretary for DIB meeting and CISO or Associate Chief Information Officer serves as facilitator.

Step 7 if DIB approves, package is submitted to OES for ECM entry and reviews (internal and external).

OES submits the CMP into ECM with initial review going to Privacy Team via work flow structure.

Step 8 Next Step

Upon internal USDA approvals and signature of the transmittal letters, Privacy Team sends to OMB via their [ROCIS system](#) maintained by General Services Administration for review and approval. The agency can also send documents to OMB via ROCIS to queue for submission however, Privacy Team is the authorized submitter. Agency's Privacy point of contact can send email to: [julio.baez@gsa.gov](mailto:julio.baez@gsa.gov) for ROCIS access.

Step 9 upon approvals, agency prepares for submission to Federal Register. Submittal to Privacy Team for preparation of Briefing Summary and Informational memorandum.

Step 10 after public review timelines on Federal Register, post to departmental webpage for CMA and ensure all active CMA(s) are included in the annual Congressional Report to include email copy to OMB.

\* Please note – CMA renewals only require a Memorandum for Extension



### 10.0 Contacts

Contacts are identified in the table below.

Table 2. Privacy Team Contacts

<i>Name</i>	<i>Role</i>	<i>Email Address</i>
Alexander Granado	Privacy Team	alexander.granado@usda.gov
Carolyn Vakil	Privacy Team	carolyn.vakil@usda.gov

### 11.0 References

Copy of Computer Matching Guidance and Template Version 2.0 is attached to these procedures for reference.

### 12.0 Related SOPs

Related Standard Operating Procedures include the following: The System of Records Notice SOP and the Privacy Impact Assessment SOP.

### 13.0 Governing Policies or Guidelines

This guidance follows USDA policy and compliance with the *E-Government Act of 2002*, as amended, 44 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. § 1401; and OMB policies and guidance that include OMB Circulars [A-108](#), *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, and OMB Circular [A-130](#), Appendix II: *Responsibilities for Managing Personally Identifiable Information*. In addition, Departmental Regulation 3xxx-001, *Computer Matching Program Involving Personally Identifiable Information (PII)*.

### 14.0 Acronyms

- A&A      Assessment and Authorization
- ATO      Authorization to Operate
- CBA      Cost Benefit Analysis
- CIO      Chief Information Officer
- CISO     Chief Information Security Officer
- CMA      Computer Matching Agreement
- CMP      Computer Matching Program



CPO	Chief Privacy Officer
DIB	Data Integrity Board
DNP	Do Not Pay
DR	Department Regulation
ECM	Enterprise Content Manager module
OES	Office of the Executive Secretariat
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personal Identifiable Information or Personally Identifiable Information
PIV	Personal Identity Verification
PTA	Privacy Threshold Analysis
SAOP	Senior Agency Official for Privacy
SORN	System of Records Notice
SSP	System Security Plan
USDA	United States Department of Agriculture



## 16.0 Approvals and Authorization

The signatures below indicate an understanding of the purpose and content of this document by those signing it. By signing this document, they agree to this as the formal standard operating procedure and guidance for completing a CMA.

The purpose of this document is to provide a vehicle for documenting the initial planning efforts for the project. It is used to reach a satisfactory level of mutual agreement between the Program Manager and the Project Sponsors and Owners with respect to the requirements and scope of the project before significant resources are committed and expenses incurred.

I have reviewed the information contained in this document and concur:

---

Signed:

Date:

**Terence Goodman**

Director, Security Management Division, Office of the Chief Information Officer



Computer  
Matching Agreemen