



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

11.3.39

JANUARY 16, 2025

EFFECTIVE DATE

(01-16-2025)

PURPOSE

- (1) This transmits revised IRM 11.3.39, *Disclosure of Official Information, Computer Matching and Privacy Protection Act*.

MATERIAL CHANGES

- (1) Editorial changes have been made throughout this entire section to conform to the internal and management control standards and to support research in electronic media.
- (2) IRM 11.3.39.1(6) Updated **Primary Stakeholders** Removed Wage and Investment and included all IRS business units and the federal, state and local government agencies that enter into a computer matching agreement would be stakeholders.

EFFECT ON OTHER DOCUMENTS

This supersedes IRM 11.3.39 dated April 12, 2024.

AUDIENCE

All Operating Divisions and Functions.

Celia Y. Doggette
Director, Governmental Liaison, Disclosure and Safeguards

11.3.39

Computer Matching and Privacy Protection Act

Table of Contents

11.3.39.1 Program Scope and Objectives

11.3.39.1.1 Background

11.3.39.1.2 Authority

11.3.39.1.3 Roles and Responsibilities

11.3.39.1.4 Program Management and Review

11.3.39.1.5 Program Controls

11.3.39.1.6 Terms and Acronyms

11.3.39.1.7 Related Resources

11.3.39.2 Definitions

11.3.39.3 Categories of Subjects Covered by CMPPA

11.3.39.4 Matching Programs Covered by CMPPA

11.3.39.4.1 Exempt Matching Programs

11.3.39.5 Requirements for Covered Computer Matching Programs

11.3.39.5.1 Written Agreements

11.3.39.5.2 Matching Program Notice and Reporting Requirements

11.3.39.5.3 Notice to Record Subjects

11.3.39.6 Existing Matching Programs

11.3.39.1
(01-16-2025)
Program Scope and Objectives

- (1) **Purpose:** This IRM section provides an overview of and provisional guidelines for Public Law (PL) 100-503, The Computer Matching and Privacy Protection Act of 1988; hereafter referred to as CMPPA. The CMPPA amended the Privacy Act of 1974 (5 U.S.C. 552a) and adds certain protections for the subjects of Privacy Act records whose records are used in automated matching programs. These protections have been mandated to ensure:
- Procedural uniformity in carrying out matching programs.
 - Due process for subjects in order to protect their rights.
 - Oversight of matching programs through the establishment of Data Integrity Boards at each agency engaging in matching to monitor the agency's matching activity.
- (2) **Scope:** The CMPPA is codified as part of the Privacy Act (5 U.S.C. 552a) and:
- Applies primarily to all federal agencies subject to the Privacy Act.
 - Brings non-federal agencies within the ambit of the Privacy Act when they are engaging in certain types of matching activities in conjunction with a federal agency that is subject to the Privacy Act; and a federal system of records is involved in the match.
 - Applies to a broad range of federal agency computer matching activities when the objective will affect an individual's rights, benefits and/or privileges.
 - Is not intended to prevent the match of any computerized data for which there exists legal authority and which is deemed the most appropriate method of achieving a desired objective; administrative controls are established to ensure privacy, integrity and verification of data disclosed for computer matching programs.
- Note:** The CMPPA does not extend Privacy Act coverage to those not originally included.
- Note:** For additional information regarding administrative privacy controls see IRM 10.5.1.8, NIST SP 800-53 Security and Privacy Controls.
- (3) **Audience:** This IRM provides procedures applicable to all the IRS Operating Divisions and Functions.
- (4) **Policy Owner:** Data Services, under Office of Governmental Liaison, Disclosure and Safeguards (GLDS), is responsible for administering CMPPA guidelines.
- (5) **Program Owner:** Office of GLDS, under Privacy, Governmental Liaison and Disclosure (PGLD), is responsible for oversight of CMPPA guidelines.
- (6) **Primary Stakeholders:** Privacy, Governmental Liaison and Disclosure in collaboration with all IRS business units and the federal, state and local government agencies that enter into computer matching agreements with the IRS.

11.3.39.1.1
(07-19-2019)
Background

- (1) One of the forces driving the Privacy Act of 1974 into existence was congressional concern about the government's use of computer systems in which to keep records about individuals. The Act's preamble points out the possibility of automated record keeping greatly magnifying the potential harm to record subjects.

- (2) Due to the steady automation of government programs, automated records play a significant and pervasive role in federal record keeping. The CMPPA is the first amendment to the Privacy Act to address the concern of automated records impacting individual privacy by establishing protections, including public and individual notice, when information an individual provides to one government agency is matched with records from another agency for a different purpose.

11.3.39.1.2
(07-19-2019)
Authority

- (1) The following statutes contain laws that relate to or impact the CMPPA:
- Privacy Act of 1974 (5 U.S.C. 552a), as amended by the Computer Matching and Privacy Protection Act of 1988 (PL 100-503)
 - 26 U.S.C. 6103, commonly referred to as Internal Revenue Code IRC 6103, is the primary law governing the authority for disclosure of federal tax information (FTI).
 - The Freedom of Information Act (5 U.S.C. 552)
 - Paperwork Reduction Act of 1995
 - Federal Information Security Modernization Act of 2014

11.3.39.1.3
(04-12-2024)
Roles and Responsibilities

- (1) Before September 30, 1997, computer matching programs (inter- and intra-agency) subject to the CMPPA were programs administered by Governmental Liaison and Disclosure.
- (2) The **Chief Privacy Officer (CPO)** is responsible for representing the IRS as a member of the Treasury Data Integrity Board (DIB) and is the executive director responsible for the IRS Privacy Program, including statutory oversight of IRS security and confidentiality requirements for federal and state agencies receiving federal tax return and return information, collectively referred to as federal tax information (FTI).

Note: For additional information regarding functional statements and management controls see IRM 1.1.27, Organization and Staffing, Privacy, Governmental Liaison and Disclosure (PGLD).

- (3) **Privacy Policy and Compliance (PPC)** is responsible for Privacy Act oversight, ensuring the IRS implements sound policies designed to protect the identity and privacy of employees and taxpayers.
- (4) **Governmental Liaison, Disclosure and Safeguards (GLDS)** is responsible for overseeing the computer matching provisions of the CMPPA, ensuring FTI is appropriately disclosed and ensuring FTI provided to federal, state and local agencies remains confidential. Through its functions, GLDS provides administration, guidance, support and technical assistance to the IRS Business and Functional Operating Division (BOD/FOD), as owner of the records, in the development of computer matching programs, agreements, notices and reports.
- a. **Data Services** is responsible for administering the IRS matching programs covered by the CMPPA and will coordinate all activities associated with initiating and continuing matching programs subject to the CMPPA provisions within the IRS, including matches that involve internal records, including personnel records, that are subject to the CMPPA.
 - b. **Governmental Liaison** is responsible for facilitating the exchange of data and fostering partnerships with federal, state and local government

agencies to improve tax administration, in accordance with IRM 1.2.1.11.13, Policy Statement 11-98 (Formerly P-6-14), FedState Relations.

- c. **Disclosure** is responsible for providing guidance and technical assistance in determining if matching programs are subject to the computer matching provisions, and if so, provide guidance in the technical review of required documents, notices and reports.
 - d. **Safeguards** is responsible for ensuring that agencies and their contractors, who have access to FTI from the IRS maintain adequate safeguards for the protection of such information.
- (5) **Business and Functional Operating Division (BOD/FOD)**, as owner of the records, is responsible for contacting Data Services, via e-mail at *GLDS.CMPPA@irs.gov*, to coordinate and prepare notices and reports required and appropriate for CMPPA matching program participation.
 - (6) Due to the increase in the number of records systems being developed, and as IRS moves towards more cooperative activities with state and local agencies, the potential has increased that matches with non-federal agencies at the area and territory levels will also be subject to the CMPPA provisions. It is incumbent on Disclosure field personnel to become familiar with the provisions of the CMPPA so they can advise and assist with achieving compliance with the CMPPA when a covered match is identified.

11.3.39.1.4
(04-12-2024)
**Program Management
and Review**

- (1) Data Exchange and Quality Initiatives (DEQI), under Data Services, is responsible for program management, including operation and maintenance. A senior data analyst within DEQI is assigned to manage the program and coordinate all required activities with internal and external stakeholders. Program activities include, but are not limited to:
 - Draft the computer matching agreement (CMA) language.
 - Obtain the necessary reviews and approvals.
 - Ensure each agency obtains approval from its respective Data Integrity Board (DIB) for matching agreements at the federal level.
 - Review existing and proposed matching programs periodically to determine if they are subject to and in compliance with the CMPPA.
 - Complete the requirements for covered matching programs as cited in 5 U.S.C. 552a(o) Matching Agreements; (p) Verification and opportunity to contest findings and (r) Report on new systems and matching programs.
 - Prepare and coordinate program costs and reimbursement from external agencies.
 - Prepare and deliver regular program reports.
 - Provide technical support.
 - Support the CPO by preparing program documentation, assessments, reports, and briefings for submission to the DIB.
- (2) The senior data analyst will review output reports through Control-D, as well as reports received directly from IT programmers, and account for disclosures made to federal, state, and local agencies participating in one or more computer matching programs throughout each calendar year. Annual accounting reports will be made available to the IRS Safeguards for agency reviews and for IRS reporting to the Joint Committee on Taxation.

11.3.39.1.5
(04-12-2024)

Program Controls

- (1) Data Services regularly reports program status through the Director, Governmental Liaison, Disclosure, and Safeguards to the IRS CPO through weekly briefings, quarterly operation reviews, and required annual reporting.
- (2) The senior data analyst within DEQI will conduct a servicewide review annually of that year's CMPPA covered matching program activities and prepare an annual report of the matching programs for the IRS. The annual report will be submitted by the CPO to the Department of Treasury Senior Agency Official for Privacy to be included in Treasury's annual report to OMB.
- (3) An annual matching review and report is required per *OMB Circular A-108*. The report will include a list of each matching program in which the agency participated during the year. For each matching program, the report will include:
 - a. A brief description of the matching program, including the names of all participating Federal and non-Federal agencies.
 - b. Links to the matching notice.
 - c. An account of whether the agency has fully adhered to the terms of the CMA.
 - d. An account of whether all disclosures of agency records for use in the matching program continue to be justified.
 - e. An indication of whether a cost-benefit analysis was performed, the results of the cost-benefit analysis, and an explanation of why the agency proceeded with any matching program for which the results of the cost-benefit analysis did not demonstrate that the program is likely to be cost effective.
 - f. A description of any CMA that the DIB disapproved and the reasons for the disapproval.
 - g. A description of any violations of matching agreements that have been alleged or identified, and a discussion of any action taken in response.

11.3.39.1.6
(04-12-2024)

Terms and Acronyms

- (1) The following table provides acronyms that are used throughout this IRM section:

Acronym	Definition
ACA	Affordable Care Act
BOD/FOD	Business and Functional Operating Division
CMA	Computer Matching Agreement
CMPPA	Computer Matching and Privacy Protection Act of 1988
CPO	Chief Privacy Officer
DEQI	Data Exchange and Quality Initiatives
DIB	Data Integrity Board
DIFSLA	Disclosure of Information to Federal, State and Local Agencies
FA-DDX	Fostering Undergraduate Talent by Unlocking Resources for Education Act (FUTURE Act) Direct Data Exchange

Acronym	Definition
FISMA	Federal Information Security Management Act
FTI	Federal Tax Information
GLDS	Governmental Liaison, Disclosure and Safeguards
IG	Inspector General
IRC	Internal Revenue Code
IT	Information Technology
NARA	National Archives and Records Administration
OMB	Office of Management and Budget
PGLD	Privacy, Governmental Liaison and Disclosure
PL	Public Law
PPC	Privacy Policy and Compliance
RCS	Records Control Schedule
SORN	System of Records Notice
TAR	Taxpayer Address Request
TIGTA	Treasury Inspector General for Tax Administration
U.S.C.	United States Code

11.3.39.1.7
(04-12-2024)

Related Resources

- (1) IRM 1.1.27, Organization and Staffing, Privacy, Governmental Liaison and Disclosure (PGLD)
 - (2) IRM 1.2.2.12.2, Delegation Order 11-2
 - (3) IRM 1.10.1, Office of the Commissioner of Internal Revenue, Correspondence Manual
 - (4) Computer Matching Programs: *U.S. Department of The Treasury Computer Matching Programs*
 - (5) National Archives and Records Administration (NARA), IRS Records Control Schedules (RCS): *National Archives and Records Administration, IRS Records Control Schedules*
 - (6) Office of Management and Budget (OMB) Circular No. A-108, Federal Agency Responsibilities for Review, Reporting and Publication under the Privacy Act: *OMB Circular A-108*
- Note:** OMB Circular No. A-108 supplements and clarifies OMB Circular No. A-130, Managing Information as a Strategic Resource.
- (7) Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource: *OMB Circular A-130*
 - (8) Privacy Act Directives: *U.S. Department of the Treasury Privacy Directives.*

- (9) Privacy Act Reports: *U.S. Department of the Treasury Privacy Reports*
- (10) The Privacy Act Handbook: *U.S. Department of the Treasury Privacy Act Handbook*
- (11) System of Records Notices (SORNs): *U.S. Department of the Treasury SORNs*

11.3.39.2
(04-12-2024)
Definitions

- (1) **Computer Matching Agreement (CMA)** - written agreement between the source agency and the recipient agency (or non-federal agency) specifying the terms for parties engaging in a matching program. There are four types of CMAs: Establishment, Renewal, Re-establishment, and Modification.

Note: *OMB Circular A-108*, Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 23, 2016), modified the terminology for CMAs in *OMB Circular A-130*, Managing Information as a Strategic Resource (July 28, 2016), from “new” to “establishment,” from “extension” to “renewal”, from “renewal” to “re-establishment” and from “revision” to “modification.”

a. **Establishment CMA -**

- Executed when an agency initially participates in a computer matching program; the computer matching program may have been in existence prior to the CMPPA.
- Requires approval by each federal agency’s Data Integrity Board (DIB) and requires development of a cost/benefit analysis.
- OMB and Congress must be notified of the CMA according to the requirements outlined in *OMB Circular A-108*.
- Publication of the matching notice in the Federal Register is required at least 30 days prior to the effective date of the CMA.
- Expires at 18 months from the effective date but may be renewed for an additional 12 months.

b. **Renewal CMA -**

- Executed within 3 months prior to the expiration of the existing CMA (establishment or re-establishment); each party to the CMA must certify to their respective DIB, in writing, that the matching program has been conducted in compliance with the existing CMA and will be conducted without change for not more than 12 months.
- DIB Chairperson can approve without a DIB vote if no changes have been made to the existing CMA.
- OMB and Congress notification is **not** required.
- Publication of the matching notice in the Federal Register is **not** required.
- Expires at 12 months and cannot be renewed.

c. **Re-establishment CMA -**

- Executed when an agency re-establishes a matching program upon the expiration of a CMA, including the expiration of a 12-month renewal.
- Requires approval by DIB and requires development of a cost/benefit analysis.

- OMB and Congress must be notified of the CMA according to the requirements outlined in *OMB Circular A-108*.
- Publication of the matching notice in the Federal Register is required at least 30 days prior to the effective date of the Re-establishment CMA.
- Expires at 18 months but may be renewed for an additional 12 months.

d. **Modification CMA -**

- Executed when an agency makes significant modifications to the existing CMA, prior to its expiration.
- Requires approval by the DIB and requires development of a cost/benefit analysis.
- Publication of the matching notice in the Federal Register is required at least 30 days prior to the effective date of the Modified CMA.
- Expires at 18 months but may be renewed for an additional 12 months.

- (2) **Cost/benefit analysis** - the CMPPA requires a cost/benefit analysis be part of an agency's decision to conduct or participate in a matching program. It must be included in matching agreements as justification of the proposed matching program and include a "specific estimate of any savings." The analysis is also used by the DIB in the review process. Statutorily mandated matches do not have to reflect a positive cost benefit in order to be approved by the DIB.
- (3) **Data Integrity Board (DIB)** - is established at the departmental level, consists of senior agency officials and is responsible for review and approval (or disapproval) of matching agreements and proposed matching programs.
- (4) **Matching program** - is the computerized comparison of two or more automated systems of records, or of a system of records with non-federal records. The records must exist in automated form or be converted to automated form to perform the match. A single matching program may involve several matches among a number of participants.
- (5) **Non-federal agency** - is a state or local governmental agency that receives records contained in a system of records from a federal agency.
- (6) **Recipient agency** - is the federal agency (or its contractor) that receives records from a Privacy Act system of records of another federal agency or from state and/or local government to be used in a matching program.
- (7) **Source agency** - is the federal agency that discloses records from a system of records to another federal agency or to a state or local governmental agency to be used in a matching program. It can also be a non-federal agency that discloses records to a federal agency to be used in a matching program.

11.3.39.3
(07-19-2019)
**Categories of Subjects
Covered by CMPPA**

- (1) Federal benefit program applicants (individuals initially applying for benefits).
- Note:** The Congress intends that federal employees be treated as beneficiaries of a federal benefit program because of their employment by the government.
- (2) Federal benefit program beneficiaries (individuals who actually receive benefits).

11.3.39.4
(07-19-2019)
**Matching Programs
Covered by CMPPA**

- (3) Providers of services to assistance programs (those who are not the primary beneficiaries of federal benefits programs, but will derive income from them, e.g., health care providers).
 - (4) Federal employees in danger of adverse and/or disciplinary action.
- (1) Only Federal benefit programs (including programs administered by states on behalf of the federal government) providing cash or in-kind assistance to individuals are covered.
 - (2) The purpose of the match must include one or more of the following:
 - Establishing or verifying initial or continuing eligibility for federal benefit programs.
 - Verifying compliance with the requirements, either statutory or regulatory, of federal benefit programs.
 - Recouping payments or delinquent debts under federal benefit programs.
 - (3) The federal benefit program or federal system of records need not be the sole source of data for a matching program to be covered by the CMPPA provisions.
 - (4) Federal personnel or payroll record matches conducted for the purpose of, or with an intended consequence of, taking adverse financial, personnel, or disciplinary or other adverse action against federal personnel or any individual, are subject to the CMPPA. This is the case even though these matches often take place within a single agency.
 - (5) Programs using records about subjects who are not individuals as defined by 5 U.S.C. 552a(a)(2) are not covered.
 - (6) The four elements must all be present before a matching program is covered under the provisions of the CMPPA. The provisions are:
 - Computerized comparison
 - Categories of subjects
 - Federal benefit program
 - Matching purpose

11.3.39.4.1
(04-12-2024)
**Exempt Matching
Programs**

- (1) Certain matching programs are exempt from the requirements of the CMPPA. For disclosure purposes, the most pertinent exemptions are those which exclude matches done for the purposes of:
 - Tax refund offset
 - Tax administration
 - IRC 6103(d)
- (2) Although the CMPPA exempts matches performed for tax administration purposes, OMB final guidance on implementing the provisions of the CMPPA expressly states that matches for management of the IRS workforce are not included in the Act's exemption of matching program requirements for tax administration purposes.
- (3) The CMPPA does not exclude matches conducted by an agency using only records from systems of records maintained by that agency, if the purpose of

the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against federal personnel.

Note: This means that matches only using the IRS Privacy Act systems of records that will result in adverse action against the IRS workforce are not exempt from the Act's matching requirements.

- (4) Matches involving federal employees conducted by Treasury Inspector General for Tax Administration (TIGTA) are exempt from the CMPPA under the Inspector General Act of 1978, as amended by the Inspector General Empowerment Act of 2016 (PL 114-317).
- (5) See 5 U.S.C. 552a(a)(8)(B) for the complete list of exempt matches.

11.3.39.5
(04-12-2024)
**Requirements for
Covered Computer
Matching Programs**

- (1) Prior to implementing a covered matching program, the BOD/FOD must coordinate with Data Services to:
 - Develop, negotiate, execute and obtain approval of a written agreement, prepared in conformance with 5 U.S.C. 552a(o), and with the other agency or other IRS function.
 - Partner with IRS Information Technology (IT) management and staffs to determine system, programming and scheduling requirements.
 - Provide notice of the matching program to record subjects.
 - Prepare a report to Congress on the new matching program.
 - Prepare any Federal Register notice and report required (unless prepared by the recipient agency).

Caution: Matching programs involving an IRS system of records must have a published routine use covering the matching activity.

11.3.39.5.1
(04-12-2024)
Written Agreements

- (1) Pursuant to 5 U.S.C. 552a(o) Matching Agreements, no record which is contained in a system of records may be disclosed for use in a computer matching program except pursuant to a CMA between the agencies.
- (2) The IRS frequently conducts the same matching program for several different agencies; the match for each agency is considered a single matching program, thus requiring a CMA with each agency.
- (3) The type of CMA must be determined in accordance with *OMB Circular A-108* and identified in IRM 11.3.39.2.
 - a. Establishment
 - b. Renewal
 - c. Re-establishment
 - d. Modification
- (4) Data Services will coordinate with the BOD/FOD to appropriately draft and negotiate the CMA language with the other agency or other IRS function. According to the CMPPA, the CMA must specify the following:
 - a. Purpose and legal authority for conducting the program.
 - b. Justification for the program and anticipated results, including a specific estimate of any savings.

- c. Description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program.
- d. Procedures for providing individualized notice to applicants for and recipients of financial assistance or payments under federal benefits programs and applicants for and holders of positions as federal personnel at the time of the application, and notice periodically thereafter.
- e. Procedures for verifying information produced in the matching program.
- f. Procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-federal agency in the matching program.

Note: Each agency shall provide a detailed description of their record retention time frames. Refer to Document 12990, IRS Records Control Schedules (RCS), Schedule 8, Administrative and Organizational Records, Item 52, Requests for Return and Return Information Files (NARA RCS Job No. N1-058-05-2, Division of Governmental Liaison and Disclosure Records Item 52). Although many of the records covered by Schedule 8 are created and maintained by the Office of the Commissioner of the Internal Revenue Service, and specified current and predecessor offices, this schedule is intended to be functional in nature and can be used by other IRS functions.

- g. Procedures for ensuring the administrative, technical and physical security of the records matched and the results of the program.
 - h. Prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-federal agency, except where required by law or essential to the conduct of the matching program.
 - i. Information on assessments that have been made on the accuracy of the records that will be used in such a matching program.
 - j. The Comptroller General may have access to all records of a recipient agency or a non-federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.
- (5) After each party to the CMA concurs with the agreement language, the final draft will be signed by the responsible official for each agency, at least 180 days prior to scheduled implementation of the matching program. The responsible official is considered the system manager or the head of the organizational unit who has delegated authority to perform Privacy Act activities in accordance with *Treasury Directive 25-04*.
- a. See IRM 1.10.1, Office of the Commissioner of Internal Revenue, Correspondence Manual, regarding the IRS Signature Package Procedures.
 - b. See IRM 1.2.2.12.2, Delegation Order 11-2, regarding delegated authority to permit the disclosure of FTI.
- (6) Data Services will submit the CMA, signed by each party to the agreement, to the Treasury DIB, via e-mail to Privacy@treasury.gov for review and approval by the Board. In accordance with *Treasury Directive 25-06*, the Board will:

- a. Review and approve or deny the CMA for receipt or disclosure of records for matching programs to ensure compliance with all relevant statutes, regulations, and OMB guidance, including 5 U.S.C. 552a(o) Matching Agreements; and
 - b. Approve or deny the CMA no later than 60 calendar days after receipt of the CMA and submit to Data Services any questions by day 30 of the 60-day period.
- (7) Upon the Board's approval, the Treasury DIB Chairperson will sign the CMA and the Treasury DIB Liaison will return the CMA to Data Services.
 - (8) Data Services will coordinate with Treasury to report the matching program to Congress and OMB, if required and per *OMB Circular A-108* guidance.

Note: The recipient agency (or source agency in a matching program where a non-federal agency is the recipient agency) is responsible for notifying and reporting to Congress and OMB of the matching program; this action must occur at the agency level, rather than the sub-agency, component, or program level.

- (9) When preparing the CMA, Data Services and the BOD/FOD must consider the systems of records to be used in the matching program. The routine use cited in the existing system notice must encompass the proposed matching program. If not, the system notice must be republished to modify the routine use statement prior to submitting the CMA for review by the Treasury DIB.
- (10) In addition, the data resulting from the matching program must be considered. If the data match results in a new system of records, then a new system notice must also be published.
- (11) The initial CMA will remain in effect for a period not to exceed 18 months. During the last 90 days of the existing CMA, the parties to the CMA will approve a one-time renewal, not to exceed 12 months. The renewal CMA does not require notice and reports to Congress and OMB and publication in the Federal Register.
- (12) Upon expiration of the initial CMA and one-time renewal CMA, a re-establishment CMA must be secured to continue the matching program. A re-establishment CMA must be fully executed within the last 90 days of the original CMA, or renewal CMA, if applicable. The re-establishment CMA requires the same notice, reporting and publication requirements as the initial CMA. The format for the initial CMA must be used for the re-establishment CMA.

11.3.39.5.2
(04-12-2024)
**Matching Program
Notice and Reporting
Requirements**

- (1) Agencies participating in matching programs that are subject to CMPPA are required to publish a matching notice in the Federal Register **at least** 30 days prior to the establishment, re-establishment, or significant modification of the matching program. Examples of significant modifications are cited in *OMB Circular A-108*.
 - a. Generally, the recipient federal agency (or the source federal agency in a match conducted with a non-federal agency) is responsible for publishing notice of the matching program in the Federal Register. However, in matching programs involving only federal agencies, the agencies will as-

- sign responsibility. In the case of matching programs conducted with a non-federal agency, the federal agency is responsible for publishing.
- b. Notice is not required for the one-year renewal of a matching program by the agency's DIB.
- (2) Agencies are required to report to OMB and Congress any proposal to establish, re-establish, or significantly modify a matching program **at least** 30 days prior to the submission of the notice to the Federal Register for publication.
- a. If the agency is re-establishing a matching program and continuing the program past the expiration of the current CMA (including any one-year renewal approved by the DIB), the agency must report the proposal to re-establish the matching program **at least** 60 days prior to the expiration of the existing CMA.
 - b. OMB will have 30 days to review the proposal to establish, re-establish, or significantly modify a matching program and provide any comments to the agency. Advance notice to OMB and Congress is required by subsection (r) of the Privacy Act.
 - c. Submission of the report to OMB will officially start the 30-day advance review period.
- Note:** OMB's 30-day review period is separate from and will not run concurrently with the publication period in the Federal Register.
- d. The report of an established, re-established, or significantly modified matching program includes a transmittal letter, a narrative statement, a draft Federal Register notice, a CMA, and any supplementary documents.

11.3.39.5.3
(04-12-2024)
**Notice to Record
Subjects**

- (1) When the IRS is the recipient agency (or federal agency when the matching program is conducted with a non-federal agency), the IRS will notify records subjects in one of two ways, either by constructive notice or direct notice.
- a. **Constructive Notice** - the IRS will coordinate with Treasury to publish constructive notice of the matching program in the Federal Register informing record subjects of the proposed matching program and in accordance with 5 U.S.C. 552a(e) and *OMB Circular A-108*, and in the format prescribed by the *Federal Register Document Drafting Handbook*.
 - b. **Direct Notice** - the IRS will provide to each individual in the match population a direct notice of the match. This will be accomplished by a statement on an application form or by separate document. In most instances, amending the Privacy Act statement on an application form will meet CMPPA requirements.
- (2) For the IRS matching programs designed to detect fraud and/or illegal acts of agency employees, the IRS will ensure that direct notice is provided to each record subject. While Document 12011, Internal Revenue Service Ethics Handbook, universally prohibits fraud or inappropriate actions on the part of its employees, a specific notice to each record subject regarding the matching program will be provided prior to the implementation of the matching program and, at the least, an annual notice during the period the matching program is authorized.

Note: TIGTA investigations are not part of the scope of matching programs for which employees will get notice, as TIGTA's matching programs have been exempted from the CMPPA by P.L. 114-317.

- (3) Notice published in the Federal Register must contain the following information:
 - a. Name of participating agency or agencies.
 - b. Purpose of the match.
 - c. Authority for conducting the match.
 - d. Categories of records and individuals covered.
 - e. Inclusive dates of the matching program.
 - f. Address for receipt of public comment or inquiries.
- (4) The IRS must publish notices of the establishment, re-establishment or modification of a matching program in the Federal Register at least 30 days prior to conducting the matching program.

11.3.39.6
(04-12-2024)
Existing Matching Programs

- (1) Data Services maintains CMAs with approximately 60 federal, state and local agencies, initially developed for master file extract programs that were in place with government entities when the CMPPA was enacted.
- (2) The CMAs maintained by Data Services cover various matching programs involving the disclosure of FTI. For example, one matching program provides address information to enable federal agencies to locate individuals to recoup monies, while another provides income information for use in determining eligibility for federal benefit programs.
- (3) Some current matching programs include:
 - a. **Disclosure of Information to Federal, State and Local Agencies (DIFSLA) Matching Program** - IRC 6103(l)(7) authorizes the IRS to disclose certain FTI to agencies administering certain programs under the Social Security Act, the Food Stamp Act of 1977 and Title 38 United States Code (Veterans' Benefits).
 - b. **Fostering Undergraduate Talent by Unlocking Resources for Education (FUTURE) Act Direct Data Exchange (FA-DDX) Program** - IRC 6103(l)(13) authorizes the IRS to disclose to the Department of Education certain FTI for the purposes of determining eligibility for, or the amount of repayments of obligations under Income-Driven Repayment plans, with respect to loans under part D of title IV of the Higher Education Act (20 U.S.C. 1070), as amended, and determining eligibility for and the amount of federal student financial aid.
 - c. **Taxpayer Address Requests (TAR) Matching Program** - IRC 6103(m)(2) authorizes the IRS to disclose, upon written request, of a taxpayer's mailing address for use by officers, employees, or agents of a federal agency for the purpose of locating such taxpayer to collect or compromise a federal claim against the taxpayer in accordance with Title 31 U.S.C. 3711, 31 U.S.C. 3717, and 31 U.S.C. 3718.
 - d. **Verification of Household Income and Family Size for Insurance Affordability Programs and Exemptions Matching Program** - IRC 6103(l)(21) authorizes the IRS to disclose certain FTI to the Centers for Medicare and Medicaid Services (CMS), a division of the Department of Health and Human Services, as a part of the eligibility determination process for programs covered by various sections of the Patient Protec-

tion and Affordable Care Act (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), codified at 42 U.S.C. 18001 (collectively, the ACA).

- e. **Medicare Part D Matching Program** - IRC 6103(l)(7) authorizes the IRS to disclose to the Social Security Administration (SSA) certain return information for the purpose of verifying eligibility for or the correct subsidy percentage of benefits provided under the Social Security Act.
- f. **Medicare Part B Matching Program** - IRC 6103(l)(20) authorizes the IRS to disclose specified return information to SSA with respect to taxpayers whose Part B and/or prescription drug coverage insurance premium(s) will (according to the IRS records) be subject to premium subsidy adjustment pursuant to the Social Security Act for the purpose of establishing the amount of any such adjustment or increase.
- g. **The IRS Data Loss Prevention Matching Program** - The IRS has the responsibility to ensure that information is kept confidential as required by the Internal Revenue Code, the Privacy Act of 1974, the Bank Secrecy Act, Title 18 of the United States Code, the Federal Information Security Modernization Act (FISMA), and other applicable laws that require safeguarding of information. Confidential information that is sent without sufficient protection is a violation of the IRS Security Policy. The IRS matches computerized data to detect and deter breaches of security policy by IRS employees, contractors, or other individuals who have been granted access to IRS information, or to IRS equipment and resources, who send electronic communications in an unsecure and unencrypted manner.