

COMPUTER MATCHING AGREEMENTS AND THE DATA INTEGRITY BOARD

I. Purpose

This Instruction implements Department of Homeland Security (DHS or Department) Directive 262-01, "Computer Matching Agreements and the Data Integrity Board."

II. Scope

This Instruction applies to the development and approval of all Computer Matching Agreements throughout DHS.

III. References

- A. Title 5, United States Code (U.S.C.), Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended]
- B. Privacy-related memoranda issued by the Office of Management and Budget (OMB), including:
 - 1. OMB Guidance, "Privacy Act of 1974; Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988," 54 Fed. Reg. 25818 (June 19, 1989)
 - 2. OMB Circular No. A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act", 81 Fed. Reg. 94424 (Dec. 23, 2016)
- C. Computer Matching Act reports by the Government Accountability Office, including:
 - 1. GAO Report (PEMD-87-2), "Computer Matching[:] Assessing Its Costs and Benefits" (Nov. 10, 1986)
 - 2. GAO Report (GAO-14-44), "Computer Matching Act[:] OMB and Selected Agencies Need to Ensure Consistent Implementation" (Jan. 13, 2014)

D. DHS Privacy Policy Guidance Memorandum 2017-01, “DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information” (April 2017)

IV. Definitions

A. **Agency**: Any executive department, military department, government, corporation, government-controlled corporation, or other establishment in the executive branch of the Federal Government, including the Executive Office of the President, or any independent regulatory agency. 5 U.S.C § 552a(a)(1) (referring to 5 U.S.C. § 552(f)).

B. **Computer Matching Agreement (CMA)**: An agreement formalizing the sharing of information pursuant to a Matching Program, as defined and described below. See also Section VI.B.

C. **Cost-Benefit Analysis**: The process whereby the recipient agency measures the benefits of engaging in a proposed CMA and compares the benefits with the costs. Benefits may include the following: the avoidance of future improper payments (i.e., preventing future overpayments by identifying and correcting an error); and the recovery of improper payments and debts (i.e., detecting an overpayment or debt already made and the collection of the money owed to an agency). Costs may include the following: personnel costs (e.g., salaries) and computer costs related to the processing of computer matching (e.g., maintenance and use of computers at facilities).

D. **Data Integrity Board (DIB)**: Reviews and approves CMAs involving the various DHS Components on behalf of the Department. Additional responsibilities are described below in Section V.

1. **Data Integrity Board Membership**: The DIB consists of senior Department officials, designated by the Secretary of Homeland Security, including the following:

- a. Chief Privacy Officer - Chairperson¹
- b. Inspector General²
- c. Officer for Civil Rights and Civil Liberties³

¹ The Secretary of Homeland Security, as Head of the agency, is required to appoint the Chairperson of the Data Integrity Board, and the members of the Data Integrity Board, as called for by 5 U.S.C. § 552a(u)(2).

² The Inspector General is a statutory member of the Data Integrity Board as called for by, 5 U.S.C. § 552a(u)(2).

³ The Chief Privacy Officer is required to coordinate with the Officer for Civil Rights and Civil Liberties as called for by 6 U.S.C. § 142(a)(5).

- d. Chief Information Officer
- e. Deputy Component Principals:
 - (1) Deputy Director, U.S. Citizenship and Immigration Services
 - (2) Deputy Administrator, Federal Emergency Management Agency
 - (3) Deputy Director, U.S. Immigration and Customs Enforcement
 - (4) Other DHS Components may be designated principals, as the Department's matching program expands

E. **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. 5 U.S.C § 552a(a)(12).

F. **Federal Personnel:** Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits). 5 U.S.C § 552a(a)(13).

G. **Individual:** As defined by the Privacy Act, and individual is a citizen of the United States or an alien lawfully admitted for permanent residence. 5 U.S.C § 552a(a)(2).

H. **Maintain:** To maintain, collect, use, or disseminate. 5 U.S.C § 552a(a)(3).

I. **Matching Program:** Pursuant to 5 U.S.C. § 552a(a)(8), any computerized comparison of:

- 1. Two or more automated systems of records or a system of records with non-federal records for the purpose of:

- a. 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,⁴ or
 - b. Recouping payments or delinquent debts under such federal benefit programs; or
2. Two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records.

The term “**Matching Program**” does not include:

1. Matches performed to produce aggregate statistical data without any personal identifiers;
2. Matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;
3. Matches performed by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;
4. Matches of tax information:
 - a. Pursuant to section 6103(d) of the Internal Revenue Code of 1986;
 - b. For purposes of tax administration as defined in section 6103(b)(4) of such Code;
 - c. For the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or

⁴ Although this Instruction only applies to payments, grants, loans, or loan guarantees made to individuals under a federal benefit program, a CMA may cover other persons if the federal benefit program covers both individuals and others not included in the definition of individuals.

d. For the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of OMB to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;

5. Matches:

a. Using records predominantly relating to federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of OMB pursuant to subsection (v)); or

b. 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;

6. Matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of federal personnel or federal contractor personnel;

7. Matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986; or

8. Matches performed pursuant to §§ 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. 402 (x)(3), 1382 (e)(1)).

J. **Non-Federal Agency**: Any state or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program. 5 U.S.C § 552a(a)(10).

K. **Recipient Agency**: Any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program. 5 U.S.C § 552a(a)(9).

L. **Record**: Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. 5 U.S.C § 552a(a)(4).

M. **Routine Use**: With respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected. 5 U.S.C § 552a(a)(7).

- N. **Senior Department Official:** The Secretary, Deputy Secretary, Component Heads, Assistant Secretaries, Chief Privacy Officer, and their designees.
- O. **Source Agency:** Any agency that discloses records contained in a system of records to be used in a matching program, or any state or local government, or agency thereof, which discloses records to be used in a matching program. 5 U.S.C § 552a(a)(11).
- P. **Statistical Record:** A record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual. 5 U.S.C § 552a(a)(6).
- Q. **System of Records:** 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 particular assigned to the individual. 5 U.S.C § 552a(a)(5).

V. Responsibilities

- A. **All employees** comply with Directive 262-01, "Computer Matching Agreements and the Data Integrity Board," and with DHS policies and procedures for entering into CMAs.
- B. The **Data Integrity Board (DIB):**
1. Oversees and coordinates the review, approval, maintenance, reporting and compliance of all DHS CMAs with applicable laws, regulations, guidelines, and existing CMAs;
 2. Reviews, approves (by majority vote), and maintains all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with all relevant statutes, regulations, and guidelines;
 3. Reviews all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, to determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assesses the costs and benefits of such programs;
 4. Reviews all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

5. Submits an annual report, compiled by the Chief Privacy Officer, which is then submitted to the Secretary of Homeland Security and the Director of OMB, and published on the DHS website, describing the matching activities of the agency, including:

- a. Matching programs in which the agency has participated as a source agency or recipient agency;
- b. Matching agreements proposed that were disapproved by the DIB;
- c. Any changes in membership or structure of the DIB in the preceding year;
- d. The reasons for any waiver of requirements for completion and submission of a cost-benefit analysis prior to the approval of a matching program;
- e. Any violations of matching agreements that have been alleged or identified and any corrective action taken; and
- f. Any other information required by the Director of OMB to be included in such report.

6. Serves as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

7. Provides interpretation and guidance, through the Chief Privacy Officer, to DHS Components and personnel on the requirements Section VI. for matching programs; and

8. Reviews DHS recordkeeping and disposal policies⁵ and practices for matching programs to assure compliance with Section VI.

C. The **General Counsel**:

1. Reviews CMAs for legal sufficiency; and
2. Serves as Counsel to the DIB.

⁵ The DIB will ensure that the DHS CMA program efficiently and appropriately complies with recommendations and governance requirements for Department records management activities as described in DHS Directive 141-01, Records and Information Management.

D. The **DHS Headquarters Privacy Office:**

1. Establishes and maintains a list (containing web page and links) of all CMA effective dates and expirations on its DHS website.
2. Serves as the Executive Director of the DIB, tallies the votes, and provides administrative support.
3. Maintains a CMA Standard Operating Procedure, a DHS DIB Cost Benefit Analysis (CBA) Methodology, and an Internal CMA Resource Page to support DIB Members and their staff.
4. Submits the annual CMA Activity Report to the Secretary and to OMB in June.
5. Hosts the annual CMA Program Review in December.
6. Carries out any and all other responsibilities described in DHS Directive 141-01.

E. **Component Privacy Officers / Privacy Points of Contact (PPOCs):**

1. Serve as the lead, within the Component, on the implementation of this Instruction and associated Directive;
2. Advise the Deputy Component Principal, serving as a member of the DIB, on his or her formal role and in reviewing CMAs or activity of the DIB;
3. Ensure that program and system managers meet the requirements outlined in this Instruction including obtaining agreement on the CMA with representatives of other federal agencies;
4. Determine whether the proposed matching and exchange is authorized under existing Privacy Act routine uses; and
5. Work with the other agency that is a party to the CMA and the Chief Privacy Officer to resolve any issues relating to systems, security, program, policy, etc.

F. **Component Program Managers**⁶ and **System Owners**⁷:

1. Determine whether the proposed matching supports DHS and the Component's programs and initiatives;
2. Obtain agreement on the CMA, including representatives of other federal agencies;
3. Work with the Chief Privacy Officer, the Component Privacy Officer or PPOC, and counsel advising the Component to prepare drafts of all CMAs;
4. Consider the incorporation of DHS and other agency comments into the CMA (when that agency is a party to the CMA);
5. Work with the senior financial official servicing the Component to prepare and request any financial documents; and
6. Ensure that an updated CBA exists when DHS is the recipient agency.

VI. DHS CMA Procedures and Development

A. **DHS CMA Program Process**:

1. DHS Components, including those designated Component individuals listed above, will initiate the development of a CMA based on its mission needs. The DHS Component and matching party will negotiate the specific terms of the matching agreement. The DIB Executive Director coordinates the CMA negotiations, including the drafting of the CBA.

⁶ As described by DHS Policy Directive 4300A, "DHS Sensitive Systems Policy," Version 13.01, July 27, 2017, Program Managers ensure compliance with applicable federal laws and DHS policy directives governing the security, operation, maintenance, and privacy protection of information systems, information projects, and programs under their control. Program Managers are responsible for program-level Plan of Actions and Milestones (known as POA&Ms) that may impact one or more systems.

⁷ As described by DHS Policy Directive 4300A, "DHS Sensitive Systems Policy," Version 13.01, July 27, 2017, System Owners use information technology to help achieve the mission needs within their program area of responsibility. They are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security and for proper administration of security. System Owners shall be designated in writing for each system by the DHS Authorizing Official (i.e., DHS Chief Information Officer (CIO) or Component CIO).

2. Once the final terms have been agreed upon by both parties, the DIB reviews and votes on the agreement. New matching agreements have an 18-month expiration period. An approved CBA (whether generated by DHS as the Recipient partner or by the other partner when DHS is the Source) must accompany such 18-month matching agreements. Once the initial 18-month expiration period has ended, DHS may renew the agreement for 12 months, without additional review by the DIB, if renewed within 3 months prior to the expiration of the original agreement, if such program will be conducted without any change, and each party to the agreement certifies to the DIB in writing that the program has been conducted in compliance with the agreement. With such certification, the DIB may renew and approve the 12-month renewal agreement without further review. Any changes to the original agreement will require a review and vote of approval by the DIB.

3. The DIB Executive Director coordinates DIB ballot collection, congressional notices, OMB reporting, Federal Register notices, public comment resolution, and obtains the DIB Chair signature on the final agreement.

B. DHS CMA Requirements:

The Department requires that CMAs be developed and then approved by the DIB for any matching programs as defined by Privacy Act.

No record that is contained in a system of records may be disclosed to a recipient agency or non-federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-federal agency specifying:

1. The purpose and legal authority for conducting the program;
2. The justification for the program and the anticipated results, including a specific estimate of any savings;
3. A 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;
4. Procedures for providing individualized notice at the time of application, and notice periodically thereafter, as directed by the DIB, to:
 - a. Applicants for, and recipients of, financial assistance or payments under federal benefit programs; and

b. Applicants for, and holders of, positions as federal personnel, that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;

5. Procedures for verifying information produced in such matching program as required by 5 U.S.C. § 552a(p).

6. Procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-federal agency in such matching program;

7. Procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;

8. 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;

9. Procedures governing the use by a recipient agency or non-federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;

10. Information on any assessments that have been made on the accuracy of the records that will be used in such matching program; and

11. Access to all records of a recipient agency or a non-federal agency may be granted to the Comptroller General when the Comptroller General deems access necessary in order to monitor or verify compliance with the agreement.

Note: In addition to the above, DHS may include additional elements in a CMA, as long as these elements do not conflict with the Privacy Act's CMA requirements. For example, DHS customarily includes a non-discrimination clause.

A copy of each agreement entered into as outlined above:

1. Is transmitted to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Government Reform of the House of Representatives and is available upon request to the public;

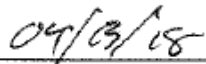
2. Is not effective until 30 days after the date on which such a copy is transmitted to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Government Reform of the House of Representatives;
3. Remains in effect only for such period, not to exceed 18 months, as the DIB of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct of the matching program;
4. May be renewed for not more than 12 months at DHS's discretion, without additional review by the DIB, if renewed within 3 months prior to the expiration of such agreement, if:
 - a. Such program will be conducted without any change; and
 - b. Each party to the agreement certifies to the DIB in writing that the program has been conducted in compliance with the agreement.

VII. Questions

Address any questions or concerns regarding this Instruction to the Senior Director of Information Sharing, Safeguarding, and Security.



Philip S. Kaplan
Chief Privacy Officer



Date