

# COMPUTER MATCHING AGREEMENTS AND THE DATA INTEGRITY BOARD

---

## I. Purpose

This Directive effectuates a Data Integrity Board (DIB) for the Department of Homeland Security (DHS or Department), and provides policies for engaging in and approving Computer Matching Agreements (CMAs) that fall under the Privacy Act of 1974, as amended (5 U.S.C. § 552a).

## II. Scope

This Directive applies throughout DHS.

## III. Authorities

- A. Title 5, United States Code, Section 552a, "Records maintained on individuals" [The Privacy Act of 1974, as amended by the Computer Matching and Privacy Protection Act of 1988].
- B. Secretarial Designation Chart, DIB, designating the membership and chairmanship of the DIB.

## IV. Responsibilities

- A. The **DIB** is responsible for:
  - 1. Overseeing and coordinating computer matching activities within the Department;
  - 2. Reviewing, approving, and maintaining all written CMAs for receipt or disclosure of the Department's Privacy Act records for matching programs;
  - 3. Reviewing all matching programs in which the Department has participated during the year, as either a source or recipient agency, to determine compliance with applicable laws, regulations, guidelines, and CMAs, and to assess the costs and benefits of such programs;

4. Reviewing all recurring matching programs in which the Department has participated during the year, either as a source or recipient agency, for continued justification for such disclosures of information;
  5. Preparing an annual report of matching activities, as provided for in 5 U.S.C. § 552a(u)(3)(D), to submit to the Secretary of Homeland Security and the Director of the Office of Management and Budget (OMB), and to be made available to the public, on request, describing the matching activities of the Department, including:
    - a. Matching programs in which the agency has participated as a source agency or recipient agency;
    - b. CMAs proposed that were disapproved by the DIB;
    - c. Changes in membership or structure of the DIB in the preceding year;
    - d. Reasons for any waiver of requirements for completion and submission of a cost-benefit analysis prior to the approval of a matching program;
    - e. Alleged or identified violations of CMAs, and any corrective action taken; and
    - f. Other information required by the Director of OMB to be included in such report.
  6. Serving as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs; and providing interpretation and guidance, in conjunction with the Chief Privacy Officer and General Counsel, to Department Components on the requirements of the 5 U.S.C. § 552a which pertain to privacy protection and required procedures;
  7. Reviewing Departmental policies and procedures for the safeguarding, security, and proper disposal of records for matching programs; and
  8. Taking any other action, as required, to ensure that matching programs do not interfere with the due process rights of individuals and follow Departmental privacy policy.
- B. The **Chief Privacy Officer** is responsible for:
1. Serving as the Chairperson of the DIB;
  2. Assisting the DIB in maintaining all CMAs to which the Department or its Components are a party;

3. Preparing an annual report of matching activities, in conjunction with the DIB, as provided for in 5 U.S.C. § 552a(u)(3)(D), to submit to the Secretary of Homeland Security and the Director of OMB, and to be made available to the public, on request, describing the matching activities of the Department, as outlined in IV(A)(5)(a-f) of this Directive;
  4. Providing interpretation and guidance to Department Components and personnel on the requirements for matching programs and privacy protection, including procedures, plans, and schedules as necessary to initiate and operate matching activities;
  5. Informing the Department's senior leadership (Secretary, Deputy Secretary, Component Heads, and their designees) of the major events and plans affecting matching activities within the Department;
  6. Participating in and providing guidance to any working group established to support DIB activities and functions, together with Department staff involved in providing technical, administrative, or management support to the DIB; and
  7. Serving as the focal point for OMB and Congress on all matters pertaining to the operation and management of matching programs and the DIB.
- C. The **Component Heads** are responsible for ensuring that Departmental activities follow DHS privacy policy and standards.

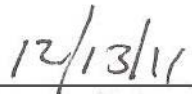
## V. Policy and Requirements

- A. Pursuant to 5 U.S.C. § 552a(o), any record contained in a system of records may only be disclosed to a recipient agency or non-federal agency for use in a computer matching program pursuant to a CMA between the source agency and the recipient agency or non-federal agency.
- B. The Department's DIB provides oversight, reviews and approves CMAs, reports on matching activities, and provides interpretation and guidance to the Department on matching activities.
- C. The Chief Privacy Officer, as Chairperson of the DIB, determines the policy, responsibilities, and management framework of the DIB, and the process for submitting CMAs for review and approval.
- D. Component Heads, or their designees, work with the Chief Privacy Officer to ensure that Department activities follow DHS privacy policy and standards, thereby enhancing the overall consistency of privacy protections across DHS.

## VI. Questions

Address any questions or concerns regarding this Directive to the Chief Privacy Officer.

  
\_\_\_\_\_  
Rafael Borrás  
Under Secretary for Management

  
\_\_\_\_\_  
Date