

**U. S. Department of the Treasury**

**Washington, D.C. 20220**

---

**The Office of the Deputy Assistant Secretary  
for  
Privacy, Transparency, & Records**

---

**Privacy Act Handbook**

**TD P 25-04**

## Table of Contents

<b>I. Background, Definitions &amp; References .....</b>	<b>6</b>
A. Introduction.....	6
B. Background.....	6
C. Definitions .....	7
D. References.....	9
<b>II. Applying Privacy Act to Records .....</b>	<b>10</b>
A. In General .....	10
B. Steps for Determining Whether the Privacy Act Applies.....	10
C. Systems Covered by the Act.....	11
D. Systems not Covered by the Act.....	11
E. Government-wide Systems of Records .....	12
F. Treasury-wide Systems of Records .....	14
<b>III. Record Keeping Under the Privacy Act.....</b>	<b>15</b>
A. General Requirements .....	15
B. First Amendment Rights.....	15
C. Information Collected from Third Parties .....	15
D. Restrictions on the Maintenance of Information about Individuals .....	16
E. Information Collected During Personal Interviews .....	16
F. Maintaining Accurate, Relevant, Timely, and Complete Records .....	17
G. System Manager Responsibilities.....	18
<b>IV. Publishing System of Records Notices.....</b>	<b>20</b>
A. General.....	20
B. When to Publish a System of Records Notice .....	20
C. Federal Register Notice Documents .....	21
D. Report to OMB and Congress Requirements .....	22
E. Format and Content of the Report .....	23
F. Timing.....	24
G. Inventory of the Department’s Systems of Records.....	25
<b>V. Privacy Act Statements, Social Security Numbers and Mailing Lists .....</b>	<b>26</b>
A. Privacy Act Statement .....	26
B. Use and Disclosure of Social Security Numbers.....	27
C. Sale or Rental of Mailing List .....	27
<b>VI. Accounting of Disclosures.....</b>	<b>28</b>

A.	In General .....	28
B.	Requirements .....	28
C.	Procedure .....	28
D.	Maintenance of Accounting Records.....	29
E.	Access to Records of Disclosure .....	29
F.	Processing Instructions .....	29
G.	Records of Accounting Not Available to the Individual .....	29
<b>VII.</b>	<b>Disclosure of Records .....</b>	<b>30</b>
A.	In General .....	30
B.	Accounting of Disclosures.....	30
C.	Disclosure Authorized Without Prior Written Consent.....	30
D.	Disclosure of Data from a Deceased Subject’s Records .....	33
<b>VIII.</b>	<b>Exemptions from the Privacy Act.....</b>	<b>34</b>
A.	In General .....	34
B.	5 U.S.C. 522a(d)(5) .....	34
C.	General Exemptions.....	34
D.	Specific Exemptions .....	35
E.	Rulemaking Requirement .....	37
<b>IX.</b>	<b>Review and Reporting Requirements.....</b>	<b>39</b>
A.	Reviews.....	39
B.	Reporting Requirements .....	<b>Error! Bookmark not defined.</b>
C.	Biennial Report.....	39
<b>X.</b>	<b>Contractors, Training, Rules of Conduct and Penalties for Non-Compliance.....</b>	<b>41</b>
A.	Contractor Personnel Subject to the Act.....	41
B.	Training.....	41
C.	Rules of Conduct .....	41
D.	Penalties for Non-Compliance.....	41
<b>XI.</b>	<b>Judicial Review .....</b>	<b>43</b>
A.	In General .....	43
B.	Conditions for Requesting Judicial Review .....	43
C.	Judicial Remedies .....	43
D.	Misrepresentation .....	44
E.	Courts Having Jurisdiction .....	44
F.	Time Limits .....	44

<b>XII. Computer Matching.....</b>	<b>45</b>
A. In General .....	45
B. Matching Program Requirements .....	45
C. Exclusions from the Definition of a Matching Program .....	46
D. Matching Notice and Publication Requirements .....	47
E. Report to OMB and Congress.....	48
F. Preparing and Executing Matching Agreements .....	48
G. Providing Due Process to Matching Subjects.....	49
H. Data Integrity Board Approval Process .....	49
I. Definitions .....	49
<b>Appendix A.....</b>	<b>51</b>
A. Definitions .....	51
B. Conditions of Disclosure .....	53
C. Accounting for Certain Disclosures.....	53
D. Access to Records.....	54
E. Agency Requirements.....	54
F. Agency Rules.....	56
G. Civil Remedies.....	56
H. Rights of Legal Guardians .....	58
I. Criminal Penalties.....	58
J. General Exemptions.....	58
K. Specific Exemptions .....	58
L. Archival Records .....	59
M. Government Contractors.....	60
N. Mailing Lists.....	60
O. Matching Agreements.....	60
P. Verification and Opportunity Contest Findings .....	61
Q. Sanctions.....	62
R. Report on New Systems and Matching Programs .....	62
S. Biennial Report.....	62
T. Effect of Other Laws .....	63
U. Data Integrity Boards.....	63
V. Office of Management and Budget Responsibilities .....	64
<b>Appendix B .....</b>	<b>66</b>
A. Office of the Federal Register SORN Template – Full Notice.....	66

B. Office of the Federal Register SORN Template – Notice of Revision .....70

C. Office of the Federal Register Notice of Rescindment Template ..... **Error! Bookmark not defined.**

**Appendix C** ..... **73**

A. Preamble .....73

## I. Background, Definitions & References

### A. Introduction

The Office of Privacy, Transparency, & Records, is issuing this handbook to carry out the provisions of the Privacy Act of 1974, as amended, 5 U.S.C. 552a. The handbook establishes the Department of the Treasury's guidelines and procedures for employees who maintain, collect, use, disseminate or amend records about individuals. Questions about this handbook or the Privacy Act should be directed to the Office of Privacy, Transparency, & Records at 202-622-0755 or via email at [privacy@treasury.gov](mailto:privacy@treasury.gov). This handbook applies to all systems of records maintained by the Department of the Treasury. A system of records is "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." The term "*system of records*" is not limited to information stored on information systems and databases. In the context of the Privacy Act, the term "system" refers to any grouping of records in paper files, information systems, or other electronic or digital mediums.

### B. Background

The Privacy Act of 1974, as amended, 5 U.S.C. 552a, Public Law 93-579 ("Privacy Act" or "the Act"), provides safeguards against the misuse of records Federal agencies maintain about individuals. In general, the Act requires Federal agencies to publish information explaining how records about individuals are collected, maintained, used, and disseminated by the Federal government. Subject to certain exceptions, the Privacy Act also permits individuals to gain access to their records which are maintained in a system of records and to seek amendment of any incorrect or incomplete information contained in those records.

Broadly stated, the purpose of the Act is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance, use and disclosure of personal information about them.

The historical context of the Act is important to an understanding of its purposes. In 1974, Congress was concerned about the Watergate scandal and allegations of illegal surveillance and investigation of individuals by Federal agencies. Congress was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal information by means of a single, universal personal identifier, such as an individual's social security number.

Specifically, the Act focuses on four policy objectives:

- 1) To establish a code of "fair information practice principles" (FIPPs) that require agencies to comply with statutory norms for collection, maintenance, and dissemination of records.
- 2) To restrict disclosure of any item, collection, or grouping of information about an individual maintained by agencies.
- 3) To grant individuals increased rights of access to records maintained about them.
- 4) To grant individuals the right to seek amendment of records maintained about them upon a showing that the records are not accurate, relevant, timely or complete.

For information on the processes related to requests for notification and access, requests for amendment and reviews of denials of amendment requests please see 31 CFR Subpart 1C (§1.26 & §1.27)<sup>1</sup> which contains the Treasury Privacy Act Regulations. These topics are not covered in this Handbook to avoid redundancy.

### C. Definitions

- 1) **Access.** Furnishing to or permitting review of records or a copy of records to the subject of the records or their authorized representative. Note: There is no provision in the Privacy Act for administrative appeal from denials of access. To address this gap in the law, it is Treasury's policy to provide maximum disclosure benefits by processing requests under both the Freedom of Information Act (FOIA) and the Privacy Act, thereby extending the FOIA appeal rights to also apply to access denials.
- 2) **Accounting of Certain Disclosures.** A record which gives a description of the Privacy Act records that have been disclosed to any person or organization external to the agency, the name and mailing address of the person or agency to whom the disclosure was made, the method and purpose of the disclosure, and the date of the disclosure. An accounting does not need to be kept of intra-agency disclosures or disclosures under the Freedom of Information Act.
- 3) **Agency.** The term includes "any executive department, military department, Government corporation, Government controlled corporation or other establishment in the executive branch of the Government (including the Executive Office of the President, or any independent regulatory agency." (5 U.S.C. 552 (e))
- 4) **Alteration to a System of Records.** Any change to an existing system of records including, but not limited to, adding new routine uses or modifying routine uses; increasing or changing the number or types of individuals on whom records are maintained; expanding the type or categories of information maintained; changing the manner in which records are organized or the manner in which records are indexed or retrieved so as to change the nature or scope of those records; changing the purpose for which the information is used; changing the equipment configuration (i.e., hardware, software, or both) on which the system is operated so as to create the potential for either greater or easier access; or causing a system of records to be withdrawn, suspended, canceled, terminated, and subsequently reinstated.
- 5) **Amendment.** A correction and/or addition to a record made pursuant to a request for change by the individual who is the subject of the records. A correction includes the removal of some word, phrase, sentence, paragraph, or page from the records, or altering an incorrect statement, date, etc. Addition may mean adding material that is furnished by the subject or a statement executed by the subject. Such a statement may or may not be sworn to or affirmed. As used throughout this handbook, the term "amendment" is meant to include both correction of records or addition to a record to make it accurate.
- 6) **Appeal.** A request for review of an agency decision to refuse to grant a requested amendment of a record.
- 7) **Appellate Official.** The individual designated by the bureau pursuant to Treasury Directive (TD) 25-04 to either affirm or reverse the initial determination denying amendment of a record under the Privacy Act, when that initial determination is appealed by the requester.
- 8) **Bureau.** A unit of the Department of the Treasury (sometimes referred to in this Handbook as "Components). The bureaus of the Department of the Treasury are:

---

<sup>1</sup> Please see [Treasury Privacy Act Regulations](#) for guidance on Requests for Amendment, Review of Denials of Amendment, and Disclosure of Records.

- a) Departmental Offices (DO)
  - b) The Office of Inspector General (OIG)
  - c) Treasury Inspector General for Tax Administration (TIGTA)
  - d) Special Inspector General for the Troubled Assets Relief Program (SIGTARP)
  - e) Special Inspector General for Pandemic Recovery (SIGPR)
  - f) Alcohol and Tobacco Tax and Trade Bureau (TTB)
  - g) Office of the Comptroller of the Currency (OCC)
  - h) Bureau of Engraving and Printing (BEP)
  - i) Bureau of the Fiscal Service (FS)
  - j) Internal Revenue Service (IRS)
  - k) United States Mint (MINT)
  - l) Financial Crimes Enforcement Network (FINCEN)
- 9) **Computer Matching Program.** A procedure in which a computer is used to compare two or more automated systems of records or a system of records with a set of non-federal records to find individuals who are common to more than one system or dataset. The procedure includes all of the steps associated with the match, including obtaining the records to be matched; actual use of the computer; administrative and investigative action on any matches; and disposition of the personal records maintained in connection with the match. A single matching program may involve several matches among a number of participants.
- 10) **Department.** The Department of the Treasury, encompassing the Departmental Offices and all other Treasury bureaus.
- 11) **Determination.** An agency decision made by a Responsible Official to grant or deny access in whole or in part to a record which is part of a system of records; or to grant or deny a requested amendment of a record, in whole or in part, in a Treasury system of records.
- 12) **Disclosure.** Furnishing a record to a third party by any means of communication – written, oral, electronic, or mechanical – without the consent of the subject. This includes furnishing records pursuant to one of twelve statutory exceptions (to the consent requirement) as permitted by subsection (b) of the Act.
- 13) **Individual.** A citizen of the United States or an alien lawfully admitted for permanent residence. This definition does not include corporations, partnerships, or other business organizational entities.
- 14) **Maintain.** This term includes collecting, keeping, using, or disseminating records.
- 15) **Privacy Act Statement.** A statement contained on any form used to collect information from an individual, or on a separate form that can be retained by the individual, which specifies the statutory authority for collecting the data; indicates whether furnishing the data is mandatory or voluntary; states if there is any effect for not furnishing the data; defines the purpose for collecting the data and the primary use(s) for which it will be used; and states other probable routine uses, if any.
- 16) **Record.** As used in the Privacy Act, any item, collection, or grouping of information about an individual that is maintained by the Department of the Treasury and that contains the name, or an identifying number, symbol or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. The record may include, but is not limited to, the individual's education, financial transactions, medical history, and criminal or employment history.



- 17) **Responsible Official.** The system manager or the head of the organizational unit having immediate custody of the records and who has been delegated by the system manager to perform Privacy Act activities in accordance with TD 25-04.
- 18) **Routine Use.** The use of a record for purposes which are compatible with the purpose for which the record was collected. The compatibility requirement applies to uses of the records internally within the agency and when disclosed externally (to persons or organizations outside the agency). Internally (within the agency), this means that the agency cannot collect the records for one purpose and then use the records for an unrelated purpose without first obtaining the consent of the individual. Externally, it means the agency must list in its system of records notice all the uses to which the records will be put outside the agency. In this context disclosing the records outside the agency to another agency or person is deemed a use. The system of records notice, which the Privacy Act requires agencies to publish in the Federal Register, must contain a listing of all of the agency's external routine uses (i.e., routine disclosures outside the agency) for the records maintained in a particular system of records.
- 19) **Statistical Record.** A record in a system of records maintained for statistical research or reporting purposes only and not used in whole or part in making any determination about an identifiable individual, except as provided by 13 U.S.C. 8.
- 20) **System of Records Notice.** Notice published in the Federal Register for each system of records being maintained by an agency. The publication of this notice is required by the Privacy Act.
- 21) **System of Records.** A group of any records under the control of the Department from which information is retrieved by the name of an individual, or by some other identifying number, symbol, or assigned to an individual. This includes records maintained in paper or electronic formats.
- 22) **System Manager.** The bureau official identified in a system of records notice as the manager of a system of records; and for Government-wide systems of records, the individual designated by the agency to act on behalf of the system manager.

#### **D. References**

- 1) Privacy Act of 1974, as amended, 5 U.S.C. 552a (Pub. L. 93-579).
- 2) Department of the Treasury Privacy Act Regulations, 31 CFR Part 1, Subpart C.
- 3) Treasury Directive 25-04, "The Privacy Act of 1974, As Amended" (February 4, 2014).
- 4) Computer Matching and Privacy Protection Act of 1988 (Pub. L. 100-503).
- 5) Office of Management and Budget (OMB) Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act (December 23, 2016).
- 6) OMB Final Guidance Interpreting the Provisions of Public Law 100-503, Computer Matching and Privacy Protection Act of 1988, (June 19, 1989).
- 7) OMB Circular A-130, Management of Federal Information Resources (July 28, 2016).
- 8) Office of Personnel Management (OPM) Regulations, 5 CFR 293.311.
- 9) National Archives and Records Administration (NARA), General Records Schedule, dated September 2004.
- 10) "Document Drafting Handbook," Office of the Federal Register, NARA.
- 11) Department of Justice, Office of Information and Privacy, "Freedom of Information Act Guide & Privacy Act Overview," updated annually.
- 12) "Guidelines on Relationship between the Privacy Act of 1974 and the Debt Collection Act of 1982" (March 30, 1983).
- 13) "Department of the Treasury Security Manual," TD P 15-71 (June 17, 2011).
- 14) National Archives and Records Administration, "Privacy Act Issuances."

- 15) Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973.
- 16) Freedom of Information Act, 5 U.S.C. 552.

## **II. Applying the Privacy Act to Records**

Summary: This chapter provides the criteria for determining whether a collection of records is subject to the Privacy Act. A listing of the Government-wide systems of records is provided at the end of the chapter.

### **A. In General**

Before maintaining information about individuals, the bureau or office must determine whether the Privacy Act applies to the information. Consider whether the information will be retrieved by name or personal identifier or whether the system can be operated without retrieving the information by a personal identifier. A bureau or office that needs to make a determination regarding the application of the Privacy Act to a collection of records should contact their bureau's Privacy Officer for assistance. If a program needs help identifying its bureau's Privacy Officer, please email [Privacy@Treasury.gov](mailto:Privacy@Treasury.gov) and the Office of Privacy, Transparency, & Record's Privacy and Civil Liberties team will send you the contact information for your bureau's Privacy Officer.

The Privacy Act, unlike the FOIA, has several definitions that limit the applicability of the Act's requirements. The two major qualifications in the Act are found in the definition of "record" and "system of records," and must be carefully considered when determining whether the information is a "record" that is maintained in a Privacy Act "system of records." These qualifications are of importance when the records are in an information system or are the raw data logs generated to administer an automated system or network.

The determination that a particular set of records is subject to the Privacy Act obligates Treasury to publish a Privacy Act system of records notice in the Federal Register; develop a Privacy Act statement for each form or other point of collection that is used to collect information from an individual (a form the bureau or office can provide to individuals who orally provide information that will be maintained in a system of records); establish a means of providing the "accounting of disclosures" required by the Act; address the recordkeeping and safeguarding requirements; establish procedures for access to and amendment of the records; and if necessary, publish a rule exempting the system of records from provisions of the Act. [See [Section IV](#) of this document for guidance in publishing a Privacy Act notice.]

### **B. Steps for Determining Whether the Privacy Act Applies**

- 1) First, make a determination about whether the information meets the Privacy Act definition of a "record." It is important to note that the Privacy Act definition of this term is narrower than it is in the context of National Archives and Records Administration (NARA) records management compliance. The Privacy Act defines a record as follows:

Any item, collection, or grouping of information about an individual that is maintained by the Department and that contains the name, or an identifying number, symbol or other identifying

particular assigned to the individual, such as a finger or voice print or a photograph. The record may include, but is not limited to, the individual's education, financial transactions, medical history, and criminal or employment history.

If your information does not meet this definition of a “record,” you are not required to draft a system of records notice. Please consult with your bureau’s Privacy Officer before you reach this conclusion.

If your information does meet this definition of “record”, please proceed to step 2 below.

- 2) Second, make a determination about whether the information will be operated as a “system of records.” The Privacy Act defines a system of records as: A group of any records under the control of the Department from which information is retrieved by the name of an individual, or by some other identifying number, symbol, or particular assigned to an individual.” Names of individuals, some other identifying number, symbol, or assigned to an individual are commonly referred to as “personal identifiers.” The use of names or personal identifiers to retrieve a record determines whether the record, regardless of whether it’s an electronic or paper record, is a record maintained in a "system of records" under the requirements of the Privacy Act. If you do not retrieve records by a personal identifier (for example, you do not input a name, address, SSN, email address, or phone number into a search function in an information system), you are not required to draft and publish a system of records notice. The mere fact that the records are *capable* of retrieval by a personal identifier is not enough. Authorized users of the records must *actually* retrieve the records by a personal identifier for the Act to apply. If authorized users of the records do not actually retrieve the records by a personal identifier, you are not required to draft a system of records notice. Please consult with your bureau’s Privacy Officer before you reach this conclusion.

### **C. Systems Covered by the Act**

The following are some examples of systems of records that are covered under the Act:

- 1) A paper or electronic system of files kept by a supervisor on each employee that includes information concerning hiring, promoting, or training of each employee, filed, and retrieved by the employee’s name and/or Treasury Employee Identification Number (EMPLID).
- 2) A system of files containing information such as a contractor's personal address, experience, qualifications, references, etc., and retrieved by the individual's name.
- 3) A system of files with applications for employment that are filed and retrieved by the applicant’s name.
- 4) A system of files with applications for a grant program upon which a decision is made based on one or more personal characteristics of an individual and retrieved by a computer-generated ID number assigned to the grant applicant.
- 5) An audit trail of a system, where records are retrieved for the purposes of identifying an individual to resolve technical errors or determine program accuracy.

### **D. Systems not Covered by the Act**

The following are some examples of collections of records that are not covered under the Act:

- 1) Purely private notes maintained by a supervisor regarding employees, used as personal memory refreshers.
- 2) Folders named for each state or congressional district with no index by an individual's name.
- 3) Records filed by subject matter (e.g., "general correspondence," "employee grievances") or company names, with no separate indices which enable retrieval by an individual's name or assigned number or symbol.
- 4) A personal phone list, card index system or contact file maintained by individual employees to assist them in their work, enabling them to meet deadlines, call people in other bureaus, etc.

If the Privacy Act applies to the records, a determination should be made as to whether the records are already covered by an existing Bureau or Office-specific system of records notice (or an existing notice that could be modified to accommodate related records). A Bureau or Office-specific system of records notice is a notice that only addresses a particular Treasury Bureau or Office's use of a system of records. If an existing Bureau or Office-specific notice already exists that covers the type of records being used in a new project or program (or can be altered for that purpose), it should be used to cover the records. For example:

- a) Travel records may already be covered by an existing Bureau or Office-specific system of records notice.
- b) System of records notices that contain the same kinds of individuals, information, and routine uses, but are in different locations can easily be amended to add a new location.
- c) If there is no existing Bureau or Office-specific system of records notice that covers the records (or can be amended to cover the records), is there a "Government-wide" system of records notice that covers the records?

## **E. Government-wide Systems of Records**

Typically, a Federal agency publishes its own SORNs for the systems of records it maintains. Certain Federal agencies, however, have the subject matter expertise with respect to particular systems of records that are commonly maintained by all Federal agencies. These Federal agencies have the responsibility for using their expertise to publish one or more SORNs which are applicable to all Federal agencies on a Government-wide basis. These SORNs are referred to as "Government-wide SORNs." If a Treasury Bureau or Office maintains a system of records covered by a Government-wide SORN, they do not need to publish their own SORN to cover these records.

There are eight Federal agencies responsible for publishing Government-wide SORNs. These agencies and the respective system number, system name, and the date and cite of its publication in the Federal Register are listed below:

- 1) **Equal Employment Opportunity Commission.**
  - a) EEOC/GOVT-1 -- Equal Employment Opportunity in the Federal Government Complaint and Appeals Records. Published July 30, 2002, at 67 FR 49338.
- 2) **Environmental Protection Agency.**
  - a) EPA-GOVT-1 – Emissions Inspection and Maintenance Records for Federal Employees Parking at Federal Parking Facilities. Published October 1, 2001, at 66 FR 49947
  - b) EPA-GOVT-2 -- Federal Docket Management System (FDMS). Published March 24, 2005, at 70 FR 15086.
- 3) **DHS/Federal Emergency Management Agency.**

- a) DHS/FEMA/GOVT-1 -- National Defense Executive Reserve System, Published January 7, 2009 at 74 FR 722.
- 4) **Federal Retirement Thrift Investment Board.**
  - a) FRTIB-1 Thrift Savings Plan Records. Published: 64 FR 50092, September 15, 1999. Effective: January 3, 2000 (see 64 FR 67917, dated December 3, 1999).
- 5) **General Services Administration.**
  - a) GSA/GOVT-2 --Employment Under Commercial Activities Contracts. Published February 10, 1983 at 48 FR 6176.
  - b) GSA/GOVT-3-- Travel Charge Card Program. Published September 10, 2009, at 74 FR 46592.
  - c) GSA/GOVT-4 --Contracted Travel Service Program. Published April 25, 2008, at 73 FR 22401.
  - d) GSA/GOVT-5--Access Certificates for Electronic Services (ACES). Published April 25, 2008, at 73 FR 22380.
  - e) GSA/GOVT-6--GSA SmartPay[reg] Purchase Charge Card Program. Published April 25, 2008, at 73 FR 22376.
  - f) GSA/GOVT-7--Personal Identity Verification Identity Management System (PIV DMS). Published April 25, 2008, at 73 FR 22377.
  - g) GSA/GOVT-8--Excluded Parties List System (EPLS). Published April 25, 2008, at 73 FR 22374.
  - h) GSA/CIO-1 System name: GSA Smart Card Program. Published October 25, 2006 at 71 FR 62469 (PIV Card system).
- 6) **Department of Labor.**
  - a) DOL/GOVT-1-- Office of Worker's Compensation Programs, Federal Employees' Compensation Act Files. Published September 23, 1993, at 58 FR 49556.
  - b) DOL/GOVT-2 -- Job Corps Student Records. Published September 23, 1993, at 58 FR 49558.
- 7) **Merit Systems Protection Board.**
  - a) MSRB/GOVT-1 -- Appeal and Case Records. Published November 21, 2002 at 67 FR 70254.
- 8) **Office of Government Ethics.**
  - a) OGE/GOVT-1 -- Executive Branch Public Financial Disclosure Reports and Other Ethics Program Records. Published January 22, 2003, at 68 FR 3099.
  - b) OGE/GOVT-2 -- Confidential Statements of Employment and Financial Interests. Published January 22, 2003, at 68 FR 3101.
- 9) **Office of Special Counsel.**
  - a) OSC/Govt-1-- OSC complaint, Litigation and Political Activity Files. Published November 19, 1999, at 64 FR 63359.
- 10) **Office of Personnel Management.**
  - a) OPM/GOVT-1 General Personnel Records, December 11, 2012, 77 FR 73694, as modified by 80 FR 74815 (November 30, 2015)
  - b) OPM/GOVT-2 Employee Performance File System Records, June 19, 2006, 71 FR 35342, 35347, as modified by 80 FR 74815 (November 30, 2015)
  - c) OPM/GOVT-3 Records of Adverse Actions, Performance Based Reduction in Grade and Removal Actions, and Termination of Probationers, April 27, 2000, 65 FR 24732, as modified by 80 FR 74815 (November 30, 2015)
  - d) OPM/GOVT-5 Recruiting, Examining, and Placement Records, March 26, 2014, 79 FR 16834, as modified by 80 FR 74815 (November 30, 2015)

- e) OPM/GOVT-6 Personnel Research and Test Validation Records, June 19, 2006, 71 FR 35354, as modified by 80 FR 74815 (November 30, 2015)
- f) OPM/GOVT-7 Applicant Race, Sex, National Origin and Disability Status Records, June 19, 2006, 71 FR 35356, as modified by 80 FR 74815 (November 30, 2015)
- g) OPM/GOVT-9 File on Position Classification Appeals, Job Grading Appeals, Retained Grade or Pay Appeals, Fair Labor Standard Act (FLSA) Claims and Complaints, Federal Civilian Employee Compensation and Leave Claims, and Settlement of Accounts for Deceased Civilian Officers and Employees, October 1, 2013, 78 FR 60331, as modified by 80 FR 74815 (November 30, 2015)
- h) OPM/GOVT-10 Employee Medical File System Records, June 21, 2010, 75 FR 35099, as modified by 80 FR 74815 (November 30, 2015)

11) **Department of Transportation.**

- a) DOT/ALL-8--Employee Transportation Facilitation. Published April 11, 2000, at 65 FR 19475.

If there is no existing Bureau or Office-specific or Government-wide system of records notice that covers the records (or can be amended to cover the records), is there a “Treasury-wide” system of records notice that covers the records?

## **F. Treasury-wide Systems of Records**

Typically, Treasury Bureaus and Offices publish their own notices for systems of records they maintain that are unique to a Treasury mission. At Treasury, some systems of records are not covered by a bureau-specific or Government-wide system of records notice, but the records are of a type commonly maintained by all (or most) Treasury Bureaus and Offices. In these cases, Treasury publishes a single system of records notice to cover all Treasury Bureaus and Offices that maintain these records. These notices are referred to as [“Treasury-wide” systems of records notices](#). If a Treasury Bureau or Office maintains a system of records covered by a Treasury-wide system of records notice, they do not need to publish their own notice to cover these records.

### **III. Record Keeping Under the Privacy Act**

Summary: This chapter identifies records management issues and restrictions imposed by the Privacy Act upon the collection and maintenance of information. The general requirements imposed on a system manager by the Act are also highlighted.

#### **A. General Requirements**

The Privacy Act and Treasury Department regulations require that before an agency begins to collect information on individuals, it must realistically assess the need to maintain such information and have a plan for the collection, processing, use, storage, and disposition of information.

Each component shall establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

All employees involved in the design, development, operation, or maintenance of any system of records subject to the Privacy Act must be aware of the potential civil and criminal penalties for violating certain provisions of the Act.

#### **B. First Amendment Rights**

No Treasury Bureau or Office may maintain records describing how any individual exercises rights guaranteed by the First Amendment. First Amendment rights include, but are not limited to religious and political beliefs, freedom of speech and of the press, and freedom of assembly and petition. Although the Department generally may not maintain these records, there are three exceptions to this rule:

- 1) If the law specifically authorizes it. For instance, an individual's religious affiliation is made known when verifying contributions above a specified amount on tax returns or describing contributions to tax exempt groups of which he or she is a member.
- 2) If the individual expressly authorizes it. For example, the individual provides information regarding experience as a group leader in a political organization to demonstrate leadership skills when applying for a government position.
- 3) If the records are pertinent to and within the scope of an authorized law enforcement activity. For example, these records may be maintained pursuant to an authorized law enforcement investigation in which evidence suggests that political or religious activities may be used as a cover for illegal activities.

#### **C. Information Collected from Third Parties**

Since information collected from a third-party source could be erroneous, irrelevant, or biased, subsection (e)(2) of the Privacy Act provides that determinations which may adversely affect an individual's rights, benefits and/or privileges under a Federal program must be made on the basis of information supplied by the records subject when practicable.

Procedures should be periodically reviewed to be sure that they are consistent with subsection (e)(2) of the Privacy Act and should consider:

- 1) The nature of the program whereby information can only be gathered from third-party sources, such as employers and banks providing earning statements to the Social Security Administration and to the Internal Revenue Service;
- 2) The cost of collecting the information directly from individuals compared with the cost of collecting information from third parties;
- 3) The risk that inaccurate information could adversely affect the individual;
- 4) The need to ensure the accuracy of information supplied by the individual; and
- 5) The need to ensure the accuracy of the information supplied by the third party by consulting with the individual involved before making a determination based on the third-party information.

#### **D. Restrictions on the Maintenance of Information about Individuals**

Subsection (e)(1) provides that each agency that maintains a system of records will "maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."

- 1) The information must serve a purpose required by statute or Executive Order.
- 2) Information must be both relevant and necessary to accomplish the authorized purpose for which it was intended. To determine this, it must be established that a legitimate purpose will be served by the information being maintained consistent with the intent of the Act.
- 3) The factors considered in determining whether information is relevant and necessary may vary, depending on the needs in each specific case. Examples of some of these considerations are:
  - a) Does the information relate to the legal purpose for which the system is maintained?
  - b) What are the adverse consequences, if any, of not collecting this information?
  - c) Does information have to be used in an individually identifiable form?
  - d) Could a sampling of information be used or does information have to be collected on everyone in the system?
  - e) How long is it necessary to retain the information?
  - f) Even though the information may be relevant and necessary under the statute, is it specifically relevant and necessary only in certain areas?
- 4) The content of systems of records should be analyzed or reviewed periodically:
  - a) In connection with the initial design of a system of records; or
  - b) Whenever any change is proposed to an existing system of records; or
  - c) Whenever an individual requests deletion of information on the basis that it is not relevant and necessary. If the inclusion of this information is characteristic of the types of records collected throughout the system, but is truly not relevant and necessary, the system manager must correct the problem immediately.
- 5) Special attention should be paid to the design of an automated system. At the time of the initial design, careful consideration should be given to including only information that is specifically "relevant" and "necessary."

#### **E. Information Collected During Personal Interviews**

Special problems may be encountered when information is gathered in personal interviews or by using investigative procedures and recorded in narrative form. There is a greater risk of gathering information that is not truly relevant or necessary. Instructions to personnel should stress the following:



- 1) The use of judgment and discretion in determining the kind of information to be requested and recorded as it relates to the purpose of the investigation or inquiry.
- 2) The use of extreme caution when dealing with information that would not generally be made public by the individual involved. This information should be collected only if it can be shown that it bears a direct relationship to the purpose for its collection.
- 3) Even though a person voluntarily provides information, this in itself does not permit recording it, unless it specifically relates to the purpose for its collection.
- 4) Opinions and subjective impressions about individuals should be avoided unless they serve a purpose in the collection of the information. For example, an official may record these impressions when investigating potential crimes or when recommending further investigations. These impressions should be identified as such and, whenever possible, include factual data.

Review procedures should be set up and used by the system manager to identify any instances where irrelevant and unnecessary data may have been collected. Reviewers should be authorized to delete this information from the record, making a note that irrelevant information has been deleted during a review. Employees should be made aware of these instances so that they may better understand the importance of gathering only relevant and necessary material. Whenever the collection of irrelevant data appears to be a rather widespread problem, further guidance should be given, or other corrective actions taken if warranted.

## **F. Maintaining Accurate, Relevant, Timely, and Complete Records**

Subsection (e)(5) provides that each agency that maintains a system of records will "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." An exception to this requirement is when the agency has properly exempted a system of records from certain provisions of the Act pursuant to 5 U.S.C. 552a (j) and (k) [See [Section XI](#) of this document].

Subsection (e)(6) provides that "prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section [the FOIA], make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes." This rule does not apply to disclosures made under FOIA because the agency's obligation under FOIA is to provide access to existing records in their current form, not to create new (including modified) records. When the information is based upon statements made by others (e.g., witness statements), the nature of the information and the purpose of the collection should be clearly stated. Accuracy, relevance, completeness, and timeliness are all always essential when collecting information that will be stored in a system of records. Absolute accuracy of records maintained in a system of records is, however, not required. Any records disclosed to a person outside the agency, (except another agency) must be as accurate as appropriate for purposes of the agency which maintained the records. It may be appropriate to advise recipients that the information disclosed was accurate as of a specific date, such as the last date on which a determination was made by the agency regarding known limits on its accuracy.

There is a continuing responsibility to meet the requirements of subsections (e)(5) and (e)(6). Employees must be alert to the fact that notations made, and actions taken may have far-reaching effects on the rights of individuals. Employees must make a reasonable effort to assure that the records created will not result in any unfair determinations about any individual.

Employees who discover discrepancies should report them to the system manager so that review and appropriate action can be taken.

## **G. System Manager Responsibilities**

System managers play a key role in the operation of the system of records under their control by ensuring compliance with the Privacy Act. They act as the primary point of contact for receipt of requests for review, access, amendment, and the accounting of disclosures. System managers are also responsible for notifying the Departmental or Bureau Privacy Officer when establishing, maintaining, revising, or deleting a system of records. In addition to designing and developing the system of records, system managers are involved with initiatives for matching activities, and the disclosure and dissemination of information.

Each system manager should be aware of the requirements of the Privacy Act; OMB Circular A-130, Appendix I - "Federal Agency Responsibilities for Maintaining Records About Individuals," 61 Federal Register 6428, dated February 20, 1996; Department of the Treasury Disclosure Regulations, 31 CFR Part 1, Subpart C; and Treasury Directive 25-04 "Implementation of the Privacy Act of 1974, as Amended."

System managers are initially responsible for determining when information about individuals needs to be collected, the policy objectives to be served by the collection, and whether the collection is authorized by a statute or Executive Order. In assessing the need for the information, the system manager should consider whether the agency really needs to use information that is individually identifiable or whether a sampling procedure or other non-specific process would suffice. The assessment should also consider the financial cost associated with maintaining the information, and the risks or adverse consequences if the agency does not collect the information.

When developing a system, system managers need to be aware of the types and source(s) of the information that is relevant and necessary to meet the policy objectives to be served by the collection. Whenever a Bureau or Office collects information about an individual from third-party sources that could be used to deny a privilege, benefit or right to an individual, greater care must be taken because of the risk that information from third-party sources may be erroneous, outdated, irrelevant or biased.

System managers must work with their Bureau/Office Privacy Officer, Chief Information Officer, legal counsel, and procurement office, as necessary to:

- 1) Prescribe the policies and procedures used for maintaining the system of records which includes collection, access, storage, retention and disposal of the records;
- 2) Determine if the records qualify for exemption from certain provisions of the Privacy Act pursuant to 5 U.S.C. 552a (j) or (k) or if the records may be compiled in anticipation of litigation;
- 3) Become familiar with the Privacy Act's restrictions on contractor access to and/or maintenance of systems of records and ensure that appropriate requirements are included in solicitations and contracts;
- 4) Ensure the deployment of necessary administrative and physical controls for storing and safeguarding records to ensure the protection of the records system from unauthorized access or disclosure (e.g., physical security, personnel screening, etc.) and from physical damage or destruction;
- 5) Determine the categories or levels of employees within the agency who need to access the records for the performance of their official duties;

- 6) Determine the format or media in which the records are maintained (paper, electronic), how long the records will be maintained, and when they will be moved to a Federal Records Center (FRC) or turned over to the National Archives and Records Administration (NARA); and
- 7) Develop criteria for determining at what point the records will have satisfied the purpose for which they were collected and when and how the records will be destroyed unless already subject to a records retention schedule.

## IV. Publishing System of Records Notices

Summary: This chapter pertains to the drafting and publication of Privacy Act notices. The requirements of the Office of the *Federal Register* concerning Privacy Act notices and rulemaking documents are highlighted. The elements needed for a notice and report to OMB and Congress are explained.

### A. General

Information about individuals cannot be collected for inclusion in a system of records until Treasury publishes a notice of that system in the *Federal Register*.

A system of records may be operated exclusively by a Bureau or Office; however, Treasury's Departmental Offices is responsible for publishing the system notice in the *Federal Register*.

Each Bureau or Office is responsible for preparing the required reports and notices of proposals to establish or alter a system of records. The Bureau or Office must prepare these notices and reports in accordance with this handbook and the Office of Management and Budget Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*. The Bureau or Office must prepare, for the signature of the Deputy Assistant Secretary for Privacy, Transparency, & Records (DASPTR), all required documentation necessary for submission to: (1) the Office of the Federal Register; (2) Congress, and (3) the Office of Management and Budget.

The Bureau or Office must ensure the completion and publication in the Federal Register of a system of records notice or altered system of records notice before maintaining (if a new system of records) or continuing to maintain (if altered) the system of records. An officer or employee of a Bureau or Office who willfully maintains a system of records without meeting the notice requirements of the Act may be found guilty of a misdemeanor and fined up to \$5,000.

The public notice must be as simple and clear as possible while achieving the objective of informing the public of the nature and purpose of the system of records. Therefore, the Bureau or Office must exercise care in the tone, language, length, and amount of detail in the public notice posted in the Federal Register.

Each Bureau or Office responsible for creating a new system of records or altering an existing system of records must first have the required documentation reviewed and approved by the bureau's legal counsel (and any other Bureau or Office officials whose concurrence is required per Bureau/Office processes) before sending it to the Office of Privacy, Transparency, and Record's Privacy and Civil Liberties Team: (1) for initial review; and (2) approval of the final version of all system notices, reports, etc.

The final package the Bureau or Office sends to the Office of Privacy, Transparency, and Record's Privacy and Civil Liberties Team for signature must include a transmittal memorandum to the DASPTR from the head of the Bureau or Office establishing or altering the system of records, explaining the action taken and the reasons for the action.

### B. When to Publish a System of Records Notice

There are several different circumstances under which a notice of a system of records must be published:

- 1) When establishing or making significant/major alterations/modifications to a system of records, the Bureau or Office must publish a notice establishing or altering a system of records. This notice must include the following:

- a) A preamble and notice;
- b) A report to OMB and Congress; and
- c) If the Bureau or Office is claiming exemptions from certain Privacy Act requirements for the system, a proposed rule and a final rule must be published in the *Federal Register* as part of the rulemaking process before that change becomes effective.

[The template for drafting a notice of a new system of records can be found in Appendix B, Office of the Federal Register SORN Template – Full Notice.](#)

- 2) Modifications that require notice are those that result in:
  - a) New categories of records maintained;
  - b) New categories of individuals on whom records are maintained;
  - c) New recipients of the information not covered in the existing routine uses; or
  - d) Changes to routine uses.

The template for drafting a notice for a modified system of records can be found in [Appendix B, Office of the Federal Register SORN Template – Notice of Revision.](#)

- 3) When making minor changes to a system of records. A Bureau or Office must submit to the Office of Privacy, Transparency, & Records a notice to reflect minor modifications to an existing system of records before the changes become effective. The notice must be accompanied by a memorandum demonstrating that the modification is not significant and, therefore, does not require submission of the other documents listed in Section B.1. above.
- 4) To rescind a system of records notice. A notice may be rescinded because the system was submitted in error, is not subject to the Privacy Act, has been discontinued, or is a duplication of an existing system. If it is important that the public be informed as soon as possible of the rescindment, notice of the rescindment may be given by proper notice in the *Federal Register*. When time is not a factor, the rescindment may be part of the periodic updating of notices. Once rescinded, reinstatement of the same system will require a new system report.

Each of the above documents are required to be prepared in draft form and submitted to the Office of Privacy, Transparency, & Records, Privacy and Civil Liberties for review and approval prior to submission of the final package to the DASPTR.

A sample package of the above items is available upon request from the Office of Privacy, Transparency, & Record’s Privacy and Civil Liberties team.

The template for drafting a notice rescinding a SORN can be found in [Appendix B, Office of the Federal Register Notice of Rescindment Template.](#)

### **C. Federal Register Notice Documents**

- 1) Format and Content of a Preamble. Any document that the Department submits for publication in the *Federal Register* must comply with the requirements of the Office of the *Federal Register*’s [“Document Drafting Handbook.”](#)

The document begins with a series of headings to identify the issuing agency, the subject matter and, if appropriate, the CFR title to be amended. This is followed by the “preamble,” which explains the purpose of the document being published, but must not contain any regulatory text. The last segment is the actual Privacy Act notice for a new or altered SORN or choosing to publish a revised SORN in its entirety.

Each Privacy Act notice or rule published in the Federal Register requires a preamble to inform the reader of the basis and purpose of the notice. Please see the preamble in Appendix C, which captions and associated text as required by the Office of the Federal Register.

#### **D. Report to OMB and Congress Requirements**

- 1) **Report on New Systems (Full Notice).** The report on a new system is intended to provide an opportunity for U.S. citizens and legal permanent residents to examine the effect the new system of records might have on them. Therefore, the report must include a discussion of confidentiality and security in such system and the extent to which the creation of the system will alter or change interagency or intergovernmental relationships related to information programs. The report should contain information which will meet these objectives. In applying the report criteria, a reasonable standard should be used to avoid excessive reporting of insignificant details which would have no meaningful Privacy Act information.

A report on a new system must be submitted when the establishment of a new system of records, subject to the Privacy Act, is proposed.

The template for drafting a full notice may be found at [Appendix B, Office of the Federal Register SORN Template – Full Notice](#).

- 2) **Report on an Altered/Modified System.** The Bureau or Office must also draft a report when an alteration to an existing system meets any of the following criteria:
  - a) The alteration increases the number or changes the types of individuals on whom records are maintained. A change involving the number, rather than the types, of individuals about whom records are kept needs only to be reported when that change significantly alters the character and purpose of the system of records. Normal increases in historical files or other increases in the number of records in a file which can be attributed to normal growth patterns need not be reported. Examples of changes which do not need to be reported are increases in the cases opened because of greater efficiency; increases in the number of requests for services rendered from the public; and increases resulting from the continuous accumulation of records.
  - b) The alteration expands the type of categories of information maintained. For example, if an employee payroll file is expanded to include data on education and training, this would be considered an expansion of the type of categories of information maintained and would have to be reported.
  - c) The alteration changes the purpose for which the information is used.
  - d) The alteration changes the equipment configuration, hardware, and/or software that creates substantially greater access to the records in the system. For example, locating interactive terminals at regional offices for accessing a system formerly accessible only at the headquarters would require a report. A report is not required for a routine acquisition of equipment, as long as the use of the acquired equipment is consistent with the use of the existing system, does not involve a risk of improper access or does not cause greater access to the information. The use of automated equipment for preparing a sort or analysis of information maintained in a manual system, without creating a continuing storage or retrieval capacity, does not constitute a change in configuration.

When a change to an information technology installation, telecommunications network, or any other general changes in information collection, processing, dissemination, or storage that affects multiple systems of records is made, a single consolidated new or altered system report may be submitted with changes to existing notices and supporting documentation included in the submission.

3) The following questions may be helpful in determining if a report needs to be submitted because of significant changes to the system of records:

a) Is this information presently included in an existing system of records?

Yes \_\_\_\_ If yes, identify the system of records and answer the following questions.

No \_\_\_\_ If no, see the section about reviewing existing or creating and new SORN:

- (1) Will there be an increase or change in the number or types of individuals on whom records are maintained? If so, explain.
- (2) Will the type or categories of information maintained be expanded? If so, explain.
- (3) Will the nature or the scope of these records be changed by altering the manner in which the records are organized, indexed, retrieved, etc.? If so, explain.
- (4) Will this alter the purpose for which the information is used? If so, explain.
- (5) What is the current method of access to the system of records?
- (6) How are the records currently stored?
- (7) Will this be changed? If so, briefly explain how.

## E. Format and Content of the Report

The report consists of a narrative statement and supporting documentation for review and approval by the Office of Privacy, Transparency & Records Privacy Act Officer. The statement should refer to information in the supporting documentation rather than restating this information.

The narrative statement should be brief, typically not exceeding four single-spaced pages, and should contain the following:

1) **Introduction.** Give background information. For example, for altered system, provide information on when the system was originally established, the citation to the original notice in the *Federal Register*, and the last republication date, if different.

For a new system, state why the system is needed. Note: If no changes to existing rules are required, this fact should be stated in the Introduction. If a new system of records or an alteration to an existing system will require the publication of a proposed and final rule amending 31 CFR 1.36, this fact should be disclosed as part of the report.

- 2) **Purpose.** For a new system, explain what the system will include and how it will be used. For a revised system, explain the necessity for revision. If the system is to be automated, explain in detail why this system is being automated and on what basis that determination was made (for example, the need for rapid retrieval as a result of a time-measurement study).
- 3) **Authority.** Identify the specific statutory provision or Executive Order that authorizes the maintenance of the system of records. The Privacy Act of 1974 is not authority for maintaining a system of records.
- 4) **Probable Effect on Individual Privacy or Other Rights.** This is an evaluation of the probable or potential effect of the proposed new or altered/modified system of records on the privacy or

other personal rights of individuals. How will the proposed new or altered system of records impact an individual's privacy? For example, will the modified system result in the collection of records that could potentially result in a reduction of salary, loss of eligibility in a Federal program, or cause the individual to be subject to administrative or civil proceedings or possible incarceration because of a violation of a criminal law? If no adverse effect is anticipated, a statement should be made regarding the system's minimal effect on individual privacy.

- 5) **Security Provided for this System.** Do not limit this item to physical security. Include such things as the personnel who will have access and the title of the individual who determines the personnel access and, if applicable, the criteria for that determination. Provide a brief description of the steps taken by the agency to minimize the risk of unauthorized access to the system of records. Since a more detailed assessment of the risks and specific administrative, technical, procedural, and physical safeguards established is to be made available to the Office of Management and Budget upon request, the assessment should be accomplished now and a copy provided to the Office of Privacy, Transparency, & Records.
- 6) **Compatibility of Routine Uses of Proposed System.** Explain how each proposed routine use (i.e., disclosures outside the agency) satisfies the compatibility requirement of subsection (a)(7) of the Act. For altered systems, this requirement pertains only to any newly proposed routine uses or any routine use to which an amendment is being proposed that increases the availability of Privacy Act records or amends the manner in which the records may be used.
- 7) **Office of Management and Budget (OMB) Requirements.** Provide OMB control numbers, expiration dates, and titles of any OMB-approved information collection requirements contained in the system of records. For example:

Title/Form Control Number	Expiration Date
Suspicious Activity Report/ 1506-0001	4/30/06
TDF-90-22.47	

If the request for OMB clearance of an information collection is pending, simply state the title of the collection and the date it was submitted for OMB clearance.

## F. Timing

- 1) The timing for submitting the report, notice and proposed rule to the Office of Privacy, Transparency, & Record's Privacy Act Officer for review and approval is determined by:
  - a) the date on which the bureau proposes to issue the data collection forms and/or instructions (the report must be submitted far enough in advance (120 days is recommended; anything less than 90 days puts completion by your deadline at risk) to allow internal review and OMB approval before any data is collected and maintained in a system of records); and/or
  - b) the date on which the bureau begins to maintain information on individuals in the new or altered system (e.g., if the bureau or office is obtaining the records from another federal agency or Treasury information system, the necessary documents (e.g., modification of the existing Treasury SORN or a new (or modified) Treasury SORN for records obtained from outside Treasury) should be submitted for approval at least 90 days before the records are transferred to the new information system).
- 2) The review and approval process involve three stages:
  - a) **Departmental Review and Approval.**



- (1) **Draft Review:** Bureaus and offices should submit drafts of the report, preamble and notice, and any proposed rule to the Office of Privacy, Transparency, & Record's (PTR) Privacy Act Officer at least 120 days before the system of records is to be implemented to avoid delays.
- (2) **Final clearance in PTR and OMB/OIRA:** After the draft documents are reviewed, the bureau or office must submit final documents, along with the transmittal memo and risk assessment, to the Office of Privacy, Transparency, & Record's Privacy Act Officer no less than 120 days before the maintenance of the system of records or the date on which the alteration to the system is to be made in order to avoid delays in maintaining the records (e.g., OMB has 30 days to review SORNs and may unilaterally extend that review period for an additional 6 days; that process alone could consume up to 60 days). This permits the Office of Privacy, Transparency, & Records to conduct the administrative and legal reviews necessary before signature by the Deputy Assistant Secretary for Privacy, Transparency, & Records.
  - b) **Congressional and Office of Management and Budget review.** After the Deputy Assistant Secretary for Privacy, Transparency, & Records signs the documents, the Treasury Privacy Act Officer will submit the report, a copy of the system of records notice, and any proposed rule to Congress and the Office of Management and Budget. If OMB provides any comments or other feedback, the bureau or office must address those issues before the documents receive OMB approval for publication in the Federal Register.
  - c) **Public review and comment (no exemptions claimed).** After OMB approval, the Office for Privacy, Transparency, & Record's Privacy Act Officer will submit the OMB approved new or altered system notice for publication in the *Federal Register* no less than 30 calendar days before maintenance of records in the new system of records or implementation of proposed alterations to an existing system of records
  - d) **Public review and comment (exemptions claimed).** If a bureau plans to exempt a system of records from certain Privacy Act provisions, the proposed regulation must provide for a 30-day comment period for the public. Separate publication of the final rule follows at a future date.

## G. Inventory of the Department's Systems of Records

Treasury is no longer required to publish the existing notices of systems of records in their entirety in the Federal Register every three years. Instead, Bureau Privacy and Civil Liberties Officers are asked to review their system notices to make necessary changes as needed, in keeping with continuous monitoring requirements. Treasury bureaus must periodically review their systems of records notices to ensure that they accurately describe the system. The Office of the Federal Register compiles and publishes a complete listing of all agencies' systems of records in the Federal Register's biennial compilation of system notices.

Treasury also maintains its inventory of Privacy Act systems of records on its [Privacy Act web page](#).

## **V. Privacy Act Statements, Social Security Numbers and Mailing Lists**

Summary: This chapter explains the need for a Privacy Act statement and what that statement should contain. The chapter also discusses the use of the social security number under the Act and the prohibition on the use of mailing lists.

### **A. Privacy Act Statement**

The Privacy Act requires that whenever Treasury collects information about individuals that will be maintained in a system of records, a Privacy Act Statement is required. When individuals are asked to supply information about themselves or a family member, the individual must be informed about the reason Treasury is requesting the information, how Treasury will use it; which information must be provided and which is voluntary; and the cost or forfeiture (e.g., denied benefits) that the individual might experience in terms of money, time, lost opportunity or other measure of value if he/she does not provide all or some of the information.

This requirement applies not only to pre-printed forms such as an application for a position or a benefit, but to sign-in logs and all other documents which require an individual to disclose an identification number or some other identifying symbol. The above should also be provided verbally when information is being collected, for example, by an in person or telephone interview (except where properly exempted from provisions of the Privacy Act).

It should be noted that information collections or questionnaires which are not subject to the Privacy Act because the records are not maintained in a system of records, do not require a Privacy Act statement. The bureau collecting the information should carefully consider whether the records might be maintained in a system of records in the future before deciding to omit the Privacy Act Statement when information is collected.

The content required in a Privacy Act Statement used by a bureau to collect information from an individual may be on the form used to collect the information, on a separate form that can be retained by the individual, in a recording (if collected via telephone) or may be read verbally to the individual (e.g., for an in-person interview). The Privacy Act Statement must contain the following information:

- 1) The general or specific authority, whether granted by statute or by Executive Order of the President (including the title or subject of that statute or order and a citation to the provision that provides specific or general authority), which authorizes the solicitation of the information and whether disclosure of this information is mandatory or voluntary. Mandatory and voluntary information should be separated on the form if possible (or put on separate forms), to avoid confusion.
- 2) The principal purpose or purposes for which the information is intended to be used (e.g., to make determinations regarding the individual's suitability for employment or to receive benefit payments) should be succinctly stated to avoid deterring the individual from reading it. When describing the principal purposes for which the information is to be used, the description must include all major purposes for which the record will be used by the agency, particularly those that might be used to determine, for example, an individual's rights or benefits under a federal program.
- 3) The "routine uses" for which the agency will use the information, specific ways, or processes in which the information is employed including the persons or agencies to whom the record may be disclosed. The description of the "routine uses" in the Privacy Act Statement is based on the

routine uses in the Privacy Act notice for the system of records the agency published in the Federal Register. The “routine uses” described in the Privacy Act Statement may be a summary of the actual routine uses published in the notice, but it does need to inform individuals under what conditions the information will be disclosed outside the Department.

- 4) The effects on the individual (beneficial or adverse), if any, of not providing all or any part of the requested information. This requirement is intended to allow the individual from whom information is being sought to know the good or bad effects of providing or not providing the information. The effect should be stated in a manner consistent with the purpose for collecting the information (number 2 above).

Any new form a bureau prepares for collecting data must include the above four items if the records are maintained in a system of records. The office issuing the form is responsible for the preparation of the Privacy Act statement. Forms and questionnaires created by the bureaus must be reviewed and approved by the bureau's Privacy Act Officer.

If a form needs, but does not currently contain a statement, the bureau's Privacy Act Officer will assist in ensuring that the appropriate Privacy Act statement is included at the next printing of the data collection form.

## **B. Use and Disclosure of Social Security Numbers**

- 1) It is unlawful to deny any right, benefit, or privilege provided by law to any individual because of that individual's refusal to disclose his or her social security account number.

However, this does not apply to:

- a) Any disclosure that is required by statute; or
  - b) The disclosure of a social security number to any Federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted before that date for the purpose of verifying an identity.
- 2) Any bureau that asks an individual to disclose his or her social security account number will inform that individual:
    - a) Whether disclosure is mandatory or voluntary;
    - b) By what statutory or other authority such number is solicited; and
    - c) What uses will be made of it.

## **C. Sale or Rental of Mailing List**

An individual's name and address shall not be sold or rented by a bureau unless such action is specifically authorized by law. This is not to be construed to require the withholding of names and addresses otherwise permitted to be made public.

## **VI. Accounting of Disclosures**

Summary: This chapter discusses: when and how to account for the disclosure of Privacy Act records; when the accounting is to be made available; how to process a request for the accounting; and when bureaus are not required to provide an accounting to the individual.

### **A. In General**

When a bureau makes a disclosure (either orally or in writing) from a Privacy Act system of records, the bureau must maintain a written record accounting for the disclosure. The bureau must maintain the accounting for a period of five years from the date of the disclosure, or for the life of the record, whichever is longer.

The purposes of the accounting are: (1) to allow individuals to learn to whom the bureau disclosed their records (i.e., receiving agencies); (2) to facilitate efforts to notify receiving agencies of any corrected or disputed records (see Chapter VIII of the Handbook); and (3) to provide audit trails for subsequent reviews of agency compliance with the disclosure requirements of the Act.

No accounting is required for disclosure of records when: (1) the individual has been given access to his/her own record; (2) disclosure is made to those officers and employees of the agency that maintains the record who have a need for the record in the performance of their duties; or (3) disclosure is required by the FOIA.

### **B. Requirements**

The written record of a disclosure must contain:

- 1) A description of the record disclosed;
- 2) The name, position title, and mailing address of the person to whom the disclosure was made;
- 3) The nature or purpose of the disclosure; and
- 4) The date of the disclosure.

### **C. Procedure**

Accounting for disclosures need not be standardized throughout the Department; however, every office, division, or branch of each bureau that discloses such information, either orally or in writing, must maintain some written or electronic record of a disclosure or be able to reconstruct an accurate and complete accounting of disclosures that allows the bureau to respond to requests in a timely fashion.

The accounting must:

- 1) Be established in the least expensive and most convenient form that will permit the system manager to advise individuals, promptly upon request, of what records concerning them have been disclosed and to whom.
- 2) Provide, at a minimum, a clear description of the record disclosed, the name and address of the person or agency to whom the disclosure is made, and the date, nature, and purpose of the disclosure.
- 3) Be maintained for 5 years or until the record is destroyed. The accounting pertaining to records transferred to a Federal Records Center, unless maintained separately, shall be transferred with the records themselves.

#### **D. Maintenance of Accounting Records**

A written record of a disclosure may be maintained either with the record from which the disclosure was made, or elsewhere. However, the accounting record must be maintained in a manner that ensures retention for at least five years or for the life of the record and permits an accurate and complete response to any proper request for an accounting of all disclosures made.

If a record is maintained on magnetic tape or some other electronic format which precludes attaching a copy of the accounting, no duplicate need be prepared. However, a log shall be kept containing all the data required.

#### **E. Access to Records of Disclosure**

An individual may request access to the accounting of disclosures of his/her records by submitting a request for such accounting to the responsible official. The request must be in writing, signed by the individual, and must be for an accounting of disclosures relating to records subject to the PA. Verification of identity requirements must be met. Requests seeking access to accountings of disclosure must be specific, generally stating the particular record and/or the system of records, and the location in which the records are maintained.

#### **F. Processing Instructions**

Time limits and general processing steps for requests for access to accountings of disclosure are consistent with those provided for general access requests. The responsible official will obtain the necessary accountings and prepare a response informing the requester that the listed items represent those accountings of disclosure that are maintained and required to be made available under the PA.

No appeal rights are provided.

#### **G. Records of Accounting Not Available to the Individual**

The bureau must maintain records of disclosures which are made for law enforcement purposes, under 5 U.S.C. 552a(b)(7). However, the bureau is not required to disclose these records of disclosure to the individual if the underlying records were properly exempted under subsections (j)(2) or (k). Therefore, it is recommended that accountings of such disclosures be maintained in such a manner that they can be readily identified and segregated from other accountings of disclosures in order to prevent inadvertent release of such information to the individual. [See [Section XI](#) of this document for additional information on Privacy Act exemptions.]

## VII. Disclosure of Records

Summary: This chapter gives guidance on providing a Privacy Act record to an individual or entity outside the Department, and when disclosures can be made without the consent of the subject of the record.

### A. In General

The Act prohibits the Department from disclosing a record which is part of a system of records without obtaining the prior written consent of the subject, unless the records are otherwise authorized to be disclosed by subsection (b) of the Act.

The term “disclosure” in this chapter does not include providing information to the subject of the record when the subject has made a request for his or her records. The processing of a first party request is discussed in Chapter VII.

### B. Accounting of Disclosures

An accounting of all disclosures made from a Privacy Act system of records is required except: (1) When the disclosure is made to “those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.” This “need to know” exception authorizes the intra-agency disclosure of a record for necessary, official purposes. (2) When the disclosure is required by the FOIA.

The procedures for establishing and maintaining an accounting of disclosures are contained in Section VI of this document.

### C. Disclosure Authorized Without Prior Written Consent

The Act permits the Department to disclose information from a record which is part of a system of records without obtaining the prior written consent of the subject under certain conditions as described below:

- 1) **Disclosure within the Department.** The Department is authorized to disclose a record which is part of a system of records to an individual who is an officer or employee of the Department maintaining the record and has a need for the records in order to perform his/her official duties.
- 2) **Disclosure under the provisions of the Freedom of Information Act.** The Department is authorized to disclose a record which is part of a system of records without obtaining the prior written consent of the subject when the disclosure is required under the provisions of the FOIA.
- 3) **Routine Use.** The Department may disclose a record which is part of a system of records when this disclosure is permitted by a routine use that has been published by the Department in the Federal Register. The information cannot be released for use for a purpose other than one that is compatible with the purpose for which it was collected, and an accounting must be maintained by the unit for any disclosure outside the Department. "Compatibility" requires that the link between the purpose for collecting the information and the reason for disclosing it be more than just mere "relevance." Rather, there must be some meaningful degree of convergence between the collection of the information and its disclosure.
- 4) **Census Bureau.** The Department may disclose a record which is part of a system of records to the Bureau of the Census for the purpose of planning or conducting a census, survey, or related activity authorized by Title 13, United States Code.

- 5) **Statistical Research.** The Department may disclose a record which is part of a system of records to a recipient who has provided advanced adequate written assurance that the record will be used solely as a statistical research or reporting record. However, such a record must be transferred in a form that is not individually identifiable, without the individual's name or individual identifying number. The responsibility for ensuring that disclosed information cannot be identified with any individual rests with the official or employee disclosing the data.

For purposes of meeting the requirement stated above, adequate assurance includes:

- a) A statement of the purpose for requesting the record; and
  - b) Certification that the record in question will be used only for statistical purposes.
- 6) **National Archives.** The Department may disclose a record which is part of a system of records to the National Archives and Records Administration (NARA) as a record which has sufficient historical or other value to warrant its evaluation by the Archivist of the United States or his designee to determine whether the record has sufficient value that it should be preserved.
- 7) **Civil or Criminal Law Enforcement Activity.** The Department may disclose a record which is part of a system of records to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for the purpose of a civil or criminal law enforcement activity if:
- a) The activity is authorized by law; and
  - b) The head or a delegated official of the agency or instrumentality has:
    - (1) Made a written request to the agency which maintains the record;
    - (2) Specified the particular record or portion of a record which is desired; and
    - (3) Specified the law enforcement activity for which the record is sought.
- 8) **Health or Safety.** The Department may disclose a record which is part of a system of records to a person when the requester shows "compelling circumstances" affecting the health or safety of an individual (not necessarily limited to the subject). A senior management official must concur with the release of such information before release.
- a. Upon disclosure under the health and safety exception, the subject must be notified in writing within 5 days of the disclosure. This requirement is met when reasonable effort is made to locate the individual and mail the notification to the last known employment or home address. Notification shall include the following information: the nature of the information disclosed, the person or agency to whom it was disclosed, the date of disclosure, and the compelling circumstances justifying the disclosure. Notification shall be given by the officer who made or authorized the disclosure.
- 9) **Congress.** The Department may disclose a record which is part of a system of records to:
- a) Either House of Congress; or
  - b) To the extent of matter within its jurisdiction, any committee or subcommittee (joint or of either House) of the Congress.

If the request is a duly authorized request on behalf of Congress through a legislative committee or subcommittee pertaining to a subject within the jurisdiction of the committee or subcommittee, then the request would fall within this condition of disclosure. Any system manager receiving a request from the chair of a committee or subcommittee should contact the bureau's legal counsel prior to processing the request.

This does not include disclosure to an individual member of Congress on behalf of a constituent, which is permissible under condition of disclosure (b)(3).

- 10) **Comptroller General.** The Department may disclose a record which is part of a system of records to the Comptroller General of the United States or to his or her authorized representative when such record is requested in the course of the performance of the duties of the General Accounting Office.
- 11) **Court of Competent Jurisdiction.** The Department may disclose a record which is part of a system of records pursuant to the order of a court of competent jurisdiction.

Note, however, courts have found that a subpoena signed by the clerk or an Assistant U.S. Attorney is not an order of a court; therefore, a disclosure pursuant to a subpoena is not appropriate under subsection (b)(11) unless the order is signed by the judge of the court.

- a) For the purposes discussed in this section, a court of competent jurisdiction includes:
  - (1) A United States Federal Court;
  - (2) A quasi-judicial agency (e.g., the United States Merit Systems Protection Board); or
  - (3) The judicial system of a State, territory, or possession of the United States.

It should be noted that OMB has informally advised that agencies may disclose

Privacy Act - protected records pursuant to a state court order under subsection (b)(11), even though that court lacks personal jurisdiction over the agency. Agencies should, however, be aware that compliance with such an order might be taken by a court as acquiescence to the court's jurisdiction, notwithstanding applicable principles of sovereign immunity.

- b) **Consultation with Legal Counsel.** Before complying, or refusing to comply, with an order of a court of competent jurisdiction, the responsible official will consult with legal counsel to ensure that the proposed response is appropriate.
- c) **Notification of the Subject.** Notice shall be provided within five working days of making the records available under compulsory legal process. As soon as practicable after being served with an order of the court, the responsible official will mail a notice to the subject informing him/her that the disclosure has taken place, specifying the name and number of the case or proceeding and nature of the information sought, except in response to an ex parte order. In the case of a Grand Jury subpoena or an ex parte order, notice must be provided within five days of its becoming a matter of public record.

Such notice shall be mailed to the subject's last known place of employment or home address. One copy of the notice should be maintained in the disclosure file and one copy associated with the record disclosed, if practical. The notice will contain the following information:

- (1) Date and authority to which the court order is or was returnable;
- (2) Date of and court issuing the ex parte order;
- (3) Nature of the information sought and provided; and
- (4) Name and number of the case or proceeding.

If the disclosure is made in response to a court order from a court of competent jurisdiction or an ex parte order under 26 U.S.C. 6103(i)(1), the notice should not be given until the order becomes a matter of public record. If the order does not indicate whether it is a matter of



public record, it may be necessary to request the issuing authority to advise the Department or component when the matter becomes public so the required notice may be issued.

The notice of the issuance of a court order is not required if the system of records has been exempted from the notice requirement (5 U.S.C. 552a(e)(8)) of the Act, pursuant to 5 U.S.C. 552a(j).

- 12) **Consumer Reporting Agency in Accordance with 31 U.S.C. 3711(f).** This disclosure exception was added to the original 11 by the Debt Collection Act of 1982. It authorizes agencies to disclose bad-debt information to credit bureaus. Before doing so, however, agencies must complete a series of due process steps designed to validate the debt and to offer the individual the chance to repay it. (See 48 Fed. Reg. 15556 (1983), OMB Guidelines on Debt Collection Act.)

#### **D. Disclosure of Data from a Deceased Subject's Records**

Whenever a specific request is made for a record which is part of a system of records and such records pertain to a deceased subject, the information required shall be disclosed unless:

- 1) It contains data pertaining to someone other than the subject;
- 2) The disclosure of the record would be considered to be an unwarranted invasion of a living person's privacy; or
- 3) The withholding of the record can otherwise be legally supported.

## VIII. Exemptions from the Privacy Act

Summary: This chapter provides information about the exemptions found in the Privacy Act. It discusses the provisions from which exemptions can be claimed, as well as the procedural requirements found in the Act and how they are impacted by the Administrative Procedure Act.

### A. In General

The Privacy Act allows the head of the agency to promulgate rules to exempt any system of records from the requirement that individuals be permitted access to records pertaining to themselves, as well as exemptions from other requirements. However, no system of records is automatically exempt from any provision of the Act except for the provision found at (d)(5).

### B. 5 U.S.C. 522a(d)(5)

The first exemption, 5 U.S.C. 522a(d)(5), is frequently overlooked as it is not located with the other exemptions found in subsections (j) and (k). This exemption is special in that it provides an exemption only from the access provision.

Subsection (d)(5) states that nothing in the Act shall require an agency to grant access to any information compiled in reasonable anticipation of a civil action or proceeding. The exemption covers documents prepared in anticipation of quasi-judicial administrative hearings and was also intended to cover preliminary judicial steps.

Unlike the attorney work-product privilege under the FOIA found at 5 U.S.C. 552(b)(5), subsection (d)(5) of the Privacy Act does not cover records compiled in anticipation of criminal actions. Records of this type may be protected under exemption (j)(2) of the PA.

A distinguishing feature between this exemption and all the other Privacy Act exemptions is that subsection (d)(5) is "self-executing" since it does not require an implementing regulation in order to be effective.

### C. General Exemptions

There are two general exemptions provided by 5 U.S.C. 552a(j).

- 1) Under subsection (j) an agency may exempt an entire system of records from certain provisions of the Act if the system of records is:
  - a) Maintained by the Central Intelligence Agency; or
  - b) Maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of:
    - (1) Information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status;
    - (2) Information compiled for the purpose of criminal investigation, including reports of informants and investigators and associated with an individual; or

- (3) Reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws, from arrest or indictment through release from supervision.
- 2) Provisions exempted under subsection (j). The head of an agency may exempt a system from certain provisions of the Act but is prohibited from exempting the system of records from the following subsections of the Act:
- (b). This subsection sets forth the conditions of disclosure that are allowed without the consent of the individual to whom the record pertains.
  - (c)(1) and (2). These two subsections require accounting for certain disclosures for either 5 years or the life of the record, whichever is longer.
  - (e)(4)(A) through (F). These subsections require the publication of certain information in a system of records notice in the Federal Register.
  - (e)(6), (e)(7), (e)(9), (e)(10), and (e)(11). These subsections require that records disclosed are accurate, complete, timely and relevant for an agency's purpose; that no record is maintained regarding an individual's exercise of his/her First Amendment rights (except under certain criteria); that rules of conduct are established for the agency employees involved in the design, development, operation or maintenance of a system of records; that appropriate safeguards for a system of records are established; and that new or altered systems of records be published in the Federal Register.
  - (i). This subsection concerns the criminal penalties imposed for violation of the Act by agency employees.

#### **D. Specific Exemptions**

5 U.S.C. 552a(k) provides seven specific exemptions which may be used by an agency when the head of the agency has promulgated rules exempting the system of records from certain provisions of the Act. Unlike the exemptions found in subsection (j), these exemptions can only be applied to specific records maintained within a system of records.

- 1) Under subsection (k), any system of records may be exempted from certain provisions of the Act if the system of records is:
- a) (k)(1) "subject to the provisions of section 552(b)(1) of this title." This exemption incorporates exemption 1 of the FOIA, requiring that the records (A) be specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy, and (B) the records are in fact properly classified pursuant to such Executive Order.
  - b) (k)(2) "investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, that if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence or, prior to the effective date of this section [9/27/75], under an implied promise that the identity of the source would be held in confidence." This exemption applies to civil investigations as well as criminal investigations.

Note: The term "investigatory material" closely follows the meaning given this phrase in exemption (b)(7) of the FOIA. Therefore, the case law which interpreted "investigatory" and "law enforcement purposes" for exemption (b)(7) of FOIA should be utilized in defining those terms as they appear in subsection (k)(2) of the Act.

- c) (k)(3) "maintained in connection with providing protection services to the President of the United States or other individuals pursuant to section 3056 of Title 18." This exemption is to cover those records which are not clearly within the scope of law enforcement records covered under subsection (k)(2) but which are necessary to assure the safety of individuals protected pursuant to 18 U.S.C. 3056.
- d) (k)(4) "required by statute to be maintained and used solely as statistical records." The language of the statute suggests that the system of records which qualifies to be exempted under this provision is a system composed exclusively of records that by statute are prohibited from being used for any purposes involving the making of a determination pertaining to any right, benefit, eligibility, or entitlement of the individual to whom they pertain; not merely that the agency does not engage in such activities.
- e) (k)(5) "investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [9/27/75], under an implied promise that the identity of the source would be held in confidence." The exemption is generally applicable to source-identifying material in background employment and personnel-type investigative files.

This exemption was included in the Act to take into account the fact that the screening of personnel to assure that only those who are properly qualified and trustworthy are placed in governmental positions will, from time to time, require information to be collected under a pledge of confidentiality.

- f) (k)(6) "testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process." This provision is to permit the agency to exempt testing or examination material used to assess the qualification of an individual for appointment or promotion in the military or civilian service only if disclosure of the record would reveal information about the testing process, giving an individual unfair competitive advantage.
  - g) (k)(7) "evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [9/27/75], under an implied promise that the identity of the source would be held in confidence."
- 2) Provisions exempted under subsection (k). The head of an agency may exempt a system of records from the following subsections of the Act:
- a) (c)(3). This subsection requires an agency to make an accounting of disclosures available to an individual of his/her records, except those disclosures made under (b)(7) of the PA.
  - b) (d). This subsection gives any individual a right of access to all records pertaining to him/her.

- c) (e)(1). This subsection requires an agency to maintain only information relevant and necessary to accomplish a purpose of the agency.
- d) (e)(4)(G). This subsection requires an agency to publish a notice in the Federal Register setting forth agency procedures whereby an individual can be notified at his/her request if a system of records contains a record pertaining to the individual.
- e) (e)(4)(H). This subsection requires an agency to publish a notice in the Federal Register setting forth agency procedures that are to be used by an individual to gain access to the records pertaining to the individual and to contest the content of the records.
- f) (e)(4)(I). This subsection requires an agency to publish a notice in the Federal Register giving the categories of sources of records in the system.
- g) (f). This subsection requires an agency to establish access and amendment procedures to be used by an individual pertaining to Privacy Act records.

It should also be noted that the Act (subsection (g)(3)(A)) grants courts the authority to review requested records in camera when a subsection (k) exemption is used to deny access. Further, when processing a request under this Act, several courts have held that reasonable segregation of the records is required whenever a subsection (k) exemption is invoked.

## **E. Rulemaking Requirement**

To obtain an exemption for a system of records from any requirement of the Act, the head of the agency that maintains the system must make a determination that the system falls within one of the categories of systems which are permitted to be exempted.

OMB Circular A-108 states that the term “agency” is not intended to be applied to subdivisions, offices or units within an agency. For that reason, the exemptions that are published at 31 CFR 1.36 are published under the authority of the Secretary of the Treasury or his/her delegate.

The determination is published as a rule in accordance with the requirements of section 553 of the Administrative Procedure Act. One court has found that agencies need to give the public a meaningful opportunity to comment on a proposed exemption of a system of records. If an agency fails to provide the public with a chance to comment on a proposed exemption, the agency would not be in compliance with the comment provision of the Administrative Procedures Act (APA). Agencies may not withhold records pursuant to 5 U.S.C. 552a(j) or (k) until the final rule has been declared effective.

Whenever a notice of a system of records is proposed for a system which is intended to be exempt from provisions of the PA, a proposed rulemaking is required to revise the listing of exempt systems, found at 31 CFR 1.36, "Notice of proposed rule exempting a system of records from requirements of the Privacy Act."

At the time that rules exempting the system of records from certain sections of the Privacy Act are adopted, the rule shall include the reasons why the system of records is to be exempted from a provision of 5 U.S.C. 552a.

Notices of proposed rules of exempt systems must be accompanied by a report to OMB and Congress identifying the subsections of the Act which are being exempted and describing the nature, effect, and reasons for the proposed exemption in greater detail than the notice of system of records itself.

After the proposed and final rulemaking document has the concurrence of the Director, Privacy and Civil Liberties and is signed by the Deputy Assistant Secretary for Privacy, Transparency, & Records,

the proposed and final documents are submitted to the Executive Secretary for approval in accordance with Treasury Directive 28-01. The rulemaking documents are then sent to the Federal Register for publication.

On November 21, 2000, the Department published revised regulations exempting certain systems of records from provisions of the Privacy Act (65 FR 69865).

Please contact the Office of Privacy, Transparency, & Records via [privacy@treasury.gov](mailto:privacy@treasury.gov) for assistance in drafting a notice of proposed rulemaking.

## IX. Review and Reporting Requirements

Summary: This chapter explains the reporting and review requirements found in the Act, OMB guidance and Treasury regulations.

### A. Reporting Requirements

On December 23, 2016, the Office of Management and Budget (OMB) issued Circular A-108 which noted that as is required by the Privacy Act, the Federal Information Security Management Act (FISMA), and other laws agencies have the authority to conduct periodic reviews (e.g., as part of their annual FISMA reviews) to promptly identify deficiencies, weaknesses, or risks. When compliance issues are identified, agencies are obligated to take appropriate steps to remedy them.

Components are to conduct the following reviews, with a frequency sufficient to ensure compliance and manage risks and be prepared to report the results of such reviews and the corrective action taken to resolve problems uncovered by the reviews to OMB through the Office of Privacy, Transparency, & Records:

- 1) Ensure that each contract that provides for the maintenance of a system of records on behalf of the agency to accomplish an agency function contains wording that makes the provisions of the Privacy Act enforceable on the contractor and its employees. ([5 U.S.C. 552a\(m\)\(1\)](#)).
- 2) Review the administration of the component's privacy program as part of the annual FISMA reporting process.
- 3) Ensure that all routine uses remain appropriate and that the recipient's use of the records continues to be compatible with the purpose for which the information was collected.
- 4) Ensure that each exemption claimed for a system of records pursuant to 5 U.S.C. § 552a(j) and (k) remains appropriate and necessary.
- 5) Review all matching programs in which the agency has participated during the calendar year and report to OMB by June 1.
- 6) Review the component's training practices to ensure they are sufficient and that component personnel understand the requirements of the Privacy Act, OMB guidance, the agency's implementing regulations and policies, and any job-specific requirements.
- 7) Review all SORNs to ensure they remain accurate, up-to-date, and appropriately scoped; that all SORNs are published in the Federal Register; that all SORNs include the information required by this Circular; and that all significant changes to SORNs have been reported to OMB and Congress.
- 8) As part of the review, Treasury should also assess whether it is in compliance with the requirement that agencies maintain no record describing how an individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the records are kept, or unless pertinent to and within the scope of an authorized law enforcement activity. Records should contain only such information about an individual as is relevant and necessary to accomplish a purpose that may be required by statute.

### B. Biennial Report

The Department of the Treasury no longer collects information concerning its Privacy Act activities for its biennial report to OMB. Section 3003 of the Federal Reports Elimination and Sunset Act of 1995 repealed (effective May 15, 2000) the requirement in Section 552a(s) for OMB to submit a biennial Privacy Act report to Congress.



## **X. Contractors, Training, Rules of Conduct and Penalties for Non-Compliance**

Summary: This chapter discusses requirements of the Act as they affect the relationship between Treasury and its contractors; the requirement for training; the rules of conduct required by Treasury regulations; and penalties provided by the Act.

### **A. Contractor Personnel Subject to the Act**

Government contractors and their employees who contract for the operation of a system of records to accomplish a Departmental function are governed by the provisions of the PA. All contracts should contain the standard contract requirements found at 48 CFR Ch.1, Part 24.1, to ensure compliance with the PA.

A contractor and employees are considered employees of the Department of the Treasury for the purposes of 5 U.S.C. 552a(i). However, for the purpose of disclosing Privacy Act records to government contractors, courts have held that a contractor's employees are not government employees. This then prevents a disclosure of agency records to a government contractor pursuant to 5 U.S.C. 552a(b)(1). In order for an agency to disclose Privacy Act records to a contractor, the agency must establish a "routine use" in the subject system of records, allowing the disclosure to the contractor.

The system manager is responsible for ensuring that the contractor complies with the contract requirements relating to privacy. Training and necessary clearances will precede the engagement of government contractors. Strict care will be used to ensure that they are given only the minimum access to data, which is necessary, and that they have no opportunity to access data beyond that which is intended that they access.

### **B. Training**

Each bureau shall institute a training program to instruct their employees, and employees of Government contractors covered by 5 U.S.C. 552a(m), who are involved in the design, development, operation or maintenance of any system of records, on a continuing basis with respect to the duties and responsibilities imposed on them and the rights conferred on individuals by the Privacy Act and Treasury Department regulations (31 CFR Part 1, Subpart C), including appendices A- M. The training shall provide suitable emphasis on the civil and criminal penalties imposed on the Department and individual employees for non-compliance with specified requirements of the PA.

### **C. Rules of Conduct**

Rules of conduct published at 31CFR0.216 require employees involved in the design, development, operation, or maintenance of any system of records or in the maintaining of records subject to the Privacy Act to comply with the conduct regulations delineated in the disclosure regulations at 31 CFR 1.28(b).

### **D. Penalties for Non-Compliance**

Any officer or employee of the Department of the Treasury shall be guilty of a misdemeanor and fined not more than \$5,000 for willfully:

- 1) Disclosing information, which is known to be prohibited by the PA, to any person or agency not entitled to receive it; and

2) Maintaining a system of records without meeting the notice requirements of the Act.

## XI. Judicial Review

Summary: This chapter provides an overview of the judicial remedies which are available to requesters under the Act and how a requester may gain access to the courts.

### A. In General

The right to ask for judicial review which is granted by the Act is not intended to permit a requester to use the Act as an alternative forum in which to collaterally attack information or records which have already been the subject of an administrative, quasi-judicial, or judicial action (e.g., a grievance, adverse action), or for which adequate judicial or administrative review is otherwise available.

### B. Conditions for Requesting Judicial Review

- 1) **Denial of Access to Records.** A requester may challenge a Department decision to deny access to records to which the requester considers himself/herself entitled to under the Act. This would include:
  - a) A challenge to the Department's determination to exempt a system of records from the requirement of the Act that the individual be granted access;
  - b) A challenge to the Department's refusal to grant access as a result of its interpretation of the definitions in the Act as they apply to information maintained by the Department. For example, an agency decision that a given record is not a part of a system of records as defined by the Act, and is therefore not subject to the provisions of the Act; or
  - c) A challenge to the Department's denial of access to records compiled in reasonable anticipation of a civil action or proceeding.
- 2) **Refusal to Amend a Record.** A requester may seek judicial review of the Department's determination not to amend a record when either of the following two conditions apply:
  - a) The requester has exhausted the administrative procedures established by the Department and the reviewing official has refused to amend the record; or
  - b) The requester contends that the Department has not considered the request to review the initial decision in a timely manner, or otherwise has not acted in a manner consistent with the requirements of the Act.
- 3) **Failure to Maintain a Record Accurately.** A requester may bring a civil action if he/she can show that:
  - a) The Department failed to maintain a record with such accuracy, relevance, timeliness, and completeness as is required by the Act; and
  - b) The deficiency in the record resulted in an adverse determination by the Department based on the contents of the record (i.e., a determination resulting in the individual's loss of a right, benefit, or entitlement), and the individual could reasonably have expected to avoid the adverse determination but for the deficiency in the record.
- 4) **Other Failures.** A requester may bring a civil action against the Department for any alleged failure to comply with the requirements of the Act or failure to comply with any rule published by the Department to implement the Act. However, the individual must demonstrate that:
  - a) The action was intentional and willful; and
  - b) The action had an adverse effect on the individual; and
  - c) The adverse effect was causally related to the Department's actions.

### C. Judicial Remedies

- 1) When, as a result of a de novo hearing, the court determines that an individual was improperly denied access to a record, the court may provide the following remedies:
  - a) Enjoin the Department from withholding the record; and
  - b) Order the Department to provide the records which were previously withheld to the complainant; and
  - c) Assess against the United States reasonable attorney fees and other litigation costs reasonably incurred by the complainant when the complainant has substantially prevailed in the case.
- 2) In a suit brought as a result of the Department's refusal to amend a record, when the court finds for the complainant, the court may provide the following remedies:
  - a) Order the Department or component in physical possession of the record to amend the record in accordance with the request, or in such a way as the court may direct; and
  - b) Assess against the government reasonable attorney fees and other litigation costs reasonably incurred by the complainant, in any case in which the complainant has substantially prevailed.
- 3) Remedies for Failure to Maintain an Accurate Record and Other Failures. In a suit brought against the Department for failure to maintain an accurate, complete, relevant, and timely record or for failure to observe a rule issued to implement the Act, if the court determines that the Department acted in a manner that was intentional or willful, the Government may be assessed for an amount equal to:
  - a) The actual damages sustained by the individual as a result of the Department's failure, but in no case less than \$1,000; and
  - b) The cost of the action, together with reasonable attorney fees, as determined by the court.

#### **D. Misrepresentation**

A civil action may be brought at any time within two years after the date the requester discovers a misrepresentation in those cases where the Department has:

- 1) Materially and willfully misrepresented any information required to be disclosed to the requester; and
- 2) The information that was misrepresented is relevant to establishing liability of the Department to the requester under the Act.

#### **E. Courts Having Jurisdiction**

The Act provides that the requester may bring an action to enforce any liability created under the Act in the District Court of the United States in the judicial district in which the requester resides; in which the requester has his/her principal place of business; in which the Department records are situated; or in the District of Columbia.

#### **F. Time Limits**

The time limit during which a civil action may be brought under the Act is generally limited to a period of two years from the date the cause of the action occurred (e.g., refusal to grant access, refusal to amend).

## XII. Computer Matching

Summary: This chapter provides information on the provisions of the Act relating to computer matching activities. It briefly describes how the Department implements requirements of the Act as they pertain to matching agreements, matching notices and the Data Integrity Board.

### A. In General

Congress made major changes to the Privacy Act of 1974 when it enacted the "Computer Matching and Privacy Protection Act of 1988" on October 18, 1988 (Public Law 100-503). The provisions of the Act became effective nine months after enactment and made no provisions which would allow the existing computer matches to be "grandfathered" after the effective date of the legislation.

### B. Matching Program Requirements

- 1) **Matching Programs Covered.** The Computer Matching and Privacy Protection Act (CMPPA) covers two kinds of matching programs:
  - a) Matches involving Federal benefits programs; and
  - b) Matches using records from Federal personnel or payroll systems of records.

A Federal benefits matching program is defined as any computerized comparison of 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.

A second type of matching program involves a computerized comparison of two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records.

- 2) **Computerized Comparison of Data.** The record comparison must be a computerized comparison involving records from:
  - a) Two or more automated systems of records (i.e., systems of records maintained by Federal agencies that are subject to the PA); or
  - b) A Federal agency's automated system of records and automated records maintained by a non-Federal (i.e., State or local) government agency or agent thereof. To be covered, matches of these records must be computerized.
- 3) **Categories of Subjects Covered.** The provisions of the CMPPA cover only the following categories of record subjects:
  - a) Applicants for Federal benefits programs (i.e., individuals initially applying for benefits);
  - b) Program beneficiaries (i.e., individual program participants who are currently receiving or formerly received benefits); and
  - c) Providers of services to support such programs (i.e., those who are not the primary beneficiaries, but who do receive income from the Federal programs -- health care providers, for example).
- 4) **Types of Programs Covered.** 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. State programs are not covered. Programs using records about subjects who are not individuals as defined by 5 U.S.C. 552a(a)(2) of the Privacy Act are not covered.

- 5) **Matching Purpose.** The purpose of a match must be one or more of the following:
  - a) Establishing or verifying initial or continuing eligibility for Federal benefits programs; or
  - b) Verifying compliance with the requirements (statutory or regulatory) of such programs; or
  - c) Recouping payments or delinquent debts under such Federal benefits programs.

It should be noted that all of the four elements (computerized comparison, categories of subjects, Federal benefit program, and matching purpose) must be present before a matching program is covered under the provisions of the CMPPA.

- 6) **Federal Personnel or Payroll Records Matches.** The CMPPA also includes matches comparing records from automated Federal personnel or payroll systems of records, or such records and automated records of State and local governments. Again, it should be noted that the comparison must be done by using a computer. Manual comparisons are not covered. In some instances, a covered match may take place within a single agency. For example, an agency may wish to determine whether any of its own personnel are participating in a benefit program administered by the agency and are not in compliance with the program's eligibility requirements. This internal match will certainly result in an adverse action if ineligibility is discovered. Therefore, it is covered by the requirements of the CMPPA.

### C. Exclusions from the Definition of a Matching Program

The CMPPA provides for eight exclusions to the Act and agencies operating such programs are not required to comply with the provisions of the CMPPA; however, any applicable provision of the Privacy Act must be complied with. The exclusions are:

- 1) **Statistical matches whose purpose is solely to produce aggregate data stripped of personal identifiers.** Implicitly, this match is not done to take action against specific individuals, although statistical inferences drawn from the data may have consequences for the subjects of the match as members of a class or group. The results of the match must not contain individually identifiable data.
- 2) **Statistical matches whose purpose is in support of any research or statistical project.** The results of this type match do not need to be stripped of individual identifiers, but the results cannot be used to make decisions that affect the rights, benefits or privileges of specific individuals. The data developed from these matching programs may be used to make decisions about a benefit program in general that may ultimately affect the beneficiaries.
- 3) **Pilot matches.** This is a small-scale match whose purpose is to gather benefit/cost data on which to premise a decision about engaging in a full-scale matching program. The pilot matches must be approved by the Data Integrity Board (DIB).
- 4) **Law enforcement investigative matches whose purpose is to gather evidence against a named person or persons in an existing investigation.** This exclusion is available to an agency or a component whose principal statutory function involves the enforcement of criminal laws and is eligible to exempt certain of its Privacy Act systems of records under subsection (j)(2) of the PA. The match must be used for the purpose of gathering evidence against a specific person or persons. The use of a match for a "fishing expedition" is not eligible for this exclusion.
- 5) **Tax administration matches.** This exclusion covers four categorical exclusions for matches using tax information, such as tax returns and tax return information. These matches are:
  - a) Matches done pursuant to Section 6103(d) of the Internal Revenue Code involving disclosures of taxpayer information to state tax officials;

- b) Matches done for the purposes of tax administration as defined in Section 6103(b)(4) of the Internal Revenue Code. The term "tax administration" means the administration, management, conduct, direction, and supervision of the execution and application of the internal revenue laws or related statutes (or equivalent laws and statutes of a state) and tax conventions to which the United States is a part; and the development and formulation of Federal tax policy relating to existing or proposed internal revenue laws, related statutes, and tax conventions; and includes assessment, collection, enforcement, litigation, publication, and statistical gathering functions under such laws, statutes or conventions. The Bureau of Alcohol, Tobacco, and Firearms also has collection and enforcement authority under the Internal Revenue Code, and tax administration is, therefore, a part of that component's responsibilities as well;
  - c) Tax refund offset matches done pursuant to the Deficit Reduction Act of 1984 (DEFRA) because of the due process procedures contained in DEFRA;
  - d) Tax refund offset matches conducted pursuant to statutes other than DEFRA provided OMB finds the due process provisions of those statutes substantially similar to those of DEFRA.
- 6) **Routine administrative matches using Federal personnel records.** These are matches between a Federal agency and other Federal agencies or between a Federal agency and non-Federal agencies for administrative purposes that use databases that contain records predominantly relating to Federal personnel. Non-Federal entity means a state, local government, Indian tribe, institution of higher education (IHE), for-profit entity, foreign public entity, foreign organization or nonprofit organization. Matches whose purpose is to take adverse action against Federal personnel are NOT excluded from the Act's coverage.
- 7) **Internal agency matches using only records from the agency's system of records.** This exclusion permits agencies to disseminate Privacy Act records to agency employees on an official need-to-know basis as provided in the Privacy Act under Section (b)(1).
- 8) **Background investigation and foreign counter-intelligence matches.** Matches done in the course of performing a background check for security clearance of Federal personnel or Federal contractor personnel are not covered. Matches done for the purpose of foreign counterintelligence are also excluded.

#### **D. Matching Notice and Publication Requirements**

Because the CMPPA does not itself authorize disclosures from systems of records for the purposes of conducting matching programs, agencies must justify any disclosures under section (b) of the PA. This means obtaining the written consent of the record subjects to the disclosure or relying on one of the 12 exceptions to the written consent rule. To rely on exception (b)(3), routine use, a notice of intent to disclose must be published in the Federal Register.

- 1) There are two ways in which record subjects can receive notice that their records may be matched:
  - a) By direct notice; e.g., information on the application form when they apply for a benefit or in a notice that arrives with a benefit they receive;
  - b) By constructive notice; e.g., publication of system notices, routine use disclosures, and matching programs in the Federal Register;
  - c) Agencies must publish notices of the establishment or alteration of a matching program in the Federal Register at least 30 days prior to conducting such programs. The recipient Federal agency in a match between Federal agencies or in a match in which a non-Federal agency discloses records to a Federal agency is responsible for publishing such notices. Where a state

or local agency is the recipient of records from a Federal agency's systems of records, the Federal source agency is responsible for publishing the notice. Where more than one agency is involved in a matching program, the agencies are encouraged to publish a consolidated notice; or

- d) Notices published in the Federal Register should contain the following information:
- (1) Name of participating agency or agencies;
  - (2) Purpose of the match;
  - (3) Authority for conducting the match;
  - (4) Categories of records and individuals covered;
  - (5) Inclusive dates of the matching program; and
  - (6) Address for receipt of public comment or inquiries

## **E. Report to OMB and Congress**

In addition, at least 30 days prior to the initiation of a new or substantially altered matching program, a report must be submitted to OMB and Congress. The report should contain the following information:

- 1) What alternatives to matching were considered and why a matching program was chosen;
- 2) The date the match was approved by each participating Federal agency's DIB; and
- 3) Whether a benefit/cost analysis was required and, if so, whether it projected a favorable ratio.

A copy of the Federal Register matching notice describing the match is to be made a part of the report.

## **F. Preparing and Executing Matching Agreements**

Federal agencies receiving records from or disclosing records to non-Federal agencies for use in matching programs are responsible for preparing the matching agreements and should solicit relevant data from non-Federal agencies where necessary. All matching agreements must be reviewed by bureau legal counsel before sending them to PTR for DIB review and approval (where appropriate). Bureaus should allow sufficient lead time to ensure that matching agreements can be negotiated, cleared by bureau legal counsel, and signed in time to secure DIB review and approval. Matching agreements must contain the following:

- 1) **Purpose and Legal Authority.** The Act does not provide independent authority for the operation of a matching program; therefore, a specific Federal or State statutory or regulatory basis must be given for undertaking the program.
- 2) **Justification and Expected Results.** An explanation of why the matching program is being used rather than some other administrative activity and what the results are expected to be.
- 3) **Records Description.** The Federal system(s) of records should be specifically identified. Included in this description is the number of records, the data elements to be included and the projected starting and completion dates of the matching program.
- 4) **Notice Procedures.** Describes the general and individual periodic notice procedures and states whether direct notice or constructive notice was given to the record subjects.
- 5) **Verification Procedures.** Describes the methods used by the agency to independently verify the information obtained through the matching program.
- 6) **Disposition of Matched Items.** Describes when and how the information generated by the matching program will be destroyed once the program's purposes and any legal retention requirements have been met.



- 7) **Security Procedures.** Describes the administrative, technical and physical safeguards to be used in protecting the information, commensurate with the level of sensitivity of the data.
- 8) **Records Usage, Duplication and Re-Disclosure Restrictions.** Describes any specific restrictions imposed either by the source or recipient agency to keep or use the records and when they will be returned or destroyed. In general, recipient agencies shall not subsequently disclose records obtained for a matching program and, under the terms of a matching agreement, for other purposes absent a specific statutory requirement or where the disclosure is essential to the conduct of a matching program.
- 9) **Records Accuracy Assessments.** Describes the quality of the records used in the computer match and indicates whether the records meet the standard imposed by the Privacy Act for ensuring the accuracy of the records.
- 10) **Comptroller General Access.** A statement that the Comptroller General may have access to all necessary records of a recipient agency or non-Federal agency to monitor or verify compliance with the agreement.

## **G. Providing Due Process to Matching Subjects**

The CMPPA prescribes certain due process requirements that the subjects of matching programs must be afforded when matches uncover adverse information about them.

- 1) **Verification of Adverse Information.** Agencies may not premise adverse action upon the raw results of a computer match. Any adverse information must be subject to investigation and verification. Absolute confirmation is not required, only a reasonable verification process that yields confirmatory data to the agency to take the intended action.
- 2) **Notice and Opportunity to Contest.** A subject of a computer match in which adverse information is uncovered shall be notified by the agency and given an opportunity to explain prior to any adverse action being taken.

## **H. Data Integrity Board Approval Process**

The CMPPA requires that each Federal agency that acts as either a source or recipient in a matching program establish a DIB to oversee the agency's participation. Before any component of Treasury participates in a matching program, Treasury's DIB must have evaluated the proposed match and approved the terms of the matching agreement.

The Act requires that the Board consists of senior agency officials designated by the agency head. The only two mandatory members are the Inspector General of the agency, who may not serve as Chairman, and the senior official responsible for the implementation of the PA.

The Treasury DIB is made up of six permanent representatives and three rotational representatives. The permanent members of the DIB are:

- 1) Deputy Assistant Secretary for Privacy, Transparency, & Records (Chair);
- 2) Inspector General;
- 3) Treasury Inspector General for Tax Administration;
- 4) Departmental Privacy Act Officer (Board Secretary);
- 5) Associate Chief Information Officer, Capital Planning and Information Management;
- 6) Assistant General Counsel (GLER);
- 7) Office of Chief Information Office.

## **I. Definitions**

- 1) **Constructive Notice.** The publication of system of records notices, routine use disclosures, and matching program in the Federal Register.
- 2) **Data Integrity Board.** A board established by each agency that acts as either a source or recipient in a matching program staffed by senior agency officials to oversee the agency's participation in matching programs.
- 3) **Direct Notice.** The subject of a record is provided with a notice on the application form or other document that his/her records may be matched.

## Appendix A

### § 552a. Records maintained on individuals

**(a) Definitions** - For purposes of this section--

- (1) the term "*agency*" means agency as defined in section 552(f) of this title;
- (2) the term "*individual*" means a citizen of the United States or an alien lawfully admitted for permanent residence;
- (3) the term "*maintain*" includes maintain, collect, use or disseminate;
- (4) the term "*record*" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his 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) the term "*system of records*" means 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;
- (6) the term "*statistical record*" means 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, except as provided by section 8 of Title 13;
- (7) the term "*routine use*" means, 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;
- (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,
  - (B) but does not include—
    - (i) matches performed to produce aggregate statistical data without any personal identifiers;
    - (ii) 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;
    - (iii) 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;
    - (iv) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in

section 6103(b)(4) of such Code, (III) 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 (IV) 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 the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;

(v) matches--

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or

(II) 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;

(vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

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

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

(ix) matches performed by the Secretary of Health and Human Services or the Inspector General of the Department of Health and Human Services with respect to potential fraud, waste, and abuse, including matches of a system of records with non-Federal records; or

(x) matches performed pursuant to section 3(d)(4) of the Achieving a Better Life Experience Act of 2014,

(9) the term "*recipient agency*" means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

(10) the term "*non-Federal agency*" means 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;

(11) the term "*source agency*" means any agency which 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;

(12) the term "*Federal benefit program*" means 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; and

(13) the term "*Federal personnel*" means 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).

## **(b) Conditions of Disclosure**

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be--

- (1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;
- (2) required under section 552 of this title;
- (3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;
- (4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13;
- (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;
- (6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;
- (7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;
- (8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;
- (9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;
- (10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;
- (11) pursuant to the order of a court of competent jurisdiction; or
- (12) to a consumer reporting agency in accordance with section 3711(e) of Title 31.

## **(c) Accounting for Certain Disclosures**

Each agency, with respect to each system of records under its control, shall—

- (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of--
  - (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and
  - (B) the name and address of the person or agency to whom the disclosure is made.
- (2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

- (3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and
- (4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

#### **(d) Access to Records**

Each agency that maintains a system of records shall—

- (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;
- (2) permit the individual to request amendment of a record pertaining to him and--
  - (A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and
  - (B) promptly, either--
    - (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or
    - (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official.
- (3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;
- (4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and
- (5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

#### **(e) Agency Requirements**

Each agency that maintains a system of records shall—

- (1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President;
- (2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;
- (3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual--
  - (A) the authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
  - (B) the principal purpose or purposes for which the information is intended to be used;
  - (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and
  - (D) the effects on him, if any, of not providing all or any part of the requested information.
- (4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include—
  - (A) the name and location of the system;
  - (B) the categories of individuals on whom records are maintained in the system;
  - (C) the categories of records maintained in the system;
  - (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
  - (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
  - (F) the title and business address of the agency official who is responsible for the system of records;
  - (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
  - (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
  - (I) the categories of sources of records in the system.
- (5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;
- (6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;
- (7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;
- (8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;
- (9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such

- person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;
- (10) Establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;
  - (11) At least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and
  - (12) If such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

#### **(f) Agency Rules**

In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

- (1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;
- (2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;
- (3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;
- (4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section;
- (5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record. The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

#### **(g) Civil Remedies**

- (1) Whenever any agency
  - (A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;
  - (B) refuses to comply with an individual request under subsection (d)(1) of this section;



- (C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or
  - (D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.
- (2)
- (A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.
  - (B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.
- (3)
- (A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter de novo, and may examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.
  - (B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.
- (4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of--
- (A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and
  - (B) the costs of the action together with reasonable attorney fees as determined by the court.
- (5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

## **(h) Rights of Legal Guardians**

For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

## **(i) Criminal Penalties**

- (1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.
- (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.
- (3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

## **(j) General Exemptions**

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is—

- (1) maintained by the Central Intelligence Agency; or
- (2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

## **(k) Specific Exemptions**

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of

records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is—

- (1) subject to the provisions of section 552(b)(1) of this title;
- (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;
- (3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;
- (4) required by statute to be maintained and used solely as statistical records;
- (5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;
- (6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or
- (7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

## **(l) Archival Records**

- (1) Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of Title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.
- (2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section,

except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

- (3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

#### **(m) Government Contractors**

- (1) When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.
- (2) A consumer reporting agency to which a record is disclosed under section 3711(e) of Title 31 shall not be considered a contractor for the purposes of this section.

#### **(n) Mailing Lists**

An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

#### **(o) Matching Agreements**

- (1) No record which 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-
  - (A) the purpose and legal authority for conducting the program;
  - (B) the justification for the program and the anticipated results, including a specific estimate of any savings;
  - (C) 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;
  - (D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to--
    - (i) applicants for and recipients of financial assistance or payments under Federal benefit programs; and
    - (ii) 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.

- (E) procedures for verifying information produced in such matching program as required by subsection (p);
  - (F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;
  - (G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;
  - (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) 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;
  - (J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and
  - (K) that 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.
- (2)
- (A) A copy of each agreement entered into pursuant to paragraph (1) shall--
    - (i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and
    - (ii) be available upon request to the public.
  - (B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).
  - (C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.
  - (D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (iii), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if—
    - (i) such program will be conducted without any change; and
    - (ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

**(p) Verification and Opportunity Contest Findings**

- (1) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until—
  - (A)
    - (i) the agency has independently verified the information; or
    - (ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that—

- (I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and
  - (II) there is a high degree of confidence that the information provided to the recipient agency is accurate.
- (B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and
  - (C)
    - (i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or
    - (ii) in the case of a program for which no such period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.
- (2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of--
    - (A) the amount of any asset or income involved;
    - (B) whether such individual has or had access to such asset or income for such individual's own use; and
    - (C) the period or periods when the individual had such asset or income.
  - (3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

**(q) Sanctions**

- (1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency or non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.
- (2) No source agency may renew a matching agreement unless--
  - (A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and
  - (B) the source agency has no reason to believe that the certification is inaccurate.

**(r) Report on New Systems and Matching Programs**

Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals.

**(s) Biennial Report**

Repealed by the Federal Reports Elimination and Sunset Act of 1995, Pub. L. No. 104-66, § 3003, 109 Stat. 707, 734-36 (1995), amended by Pub. L. No. 106-113, § 236, 113 Stat. 1501, 1501A-302 (1999) (changing effective date to May 15, 2000).

**(t) Effect of Other Laws**

- (1) No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section.
- (2) No agency shall rely on any exemption in this section to withhold from an individual any record which is otherwise accessible to such individual under the provisions of section 552 of this title.

**(u) Data Integrity Boards**

- (1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of such agency the agency's implementation of this section.
- (2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.
- (3) Each Data Integrity Board--
  - (A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;
  - (B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs;
  - (C) shall review 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;
  - (D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including--
    - (i) matching programs in which the agency has participated as a source agency or recipient agency;
    - (ii) matching agreements proposed under subsection (o) that were disapproved by the Board;
    - (iii) any changes in membership or structure of the Board in the preceding year;
    - (iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;
    - (v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and
    - (vi) any other information required by the Director of the Office of Management and Budget to be included in such report;

- (E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;
  - (F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;
  - (G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and
  - (H) may review and report on any agency matching activities that are not matching programs.
- (4)

- (A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.
- (B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the Office of Management and Budget, that a cost-benefit analysis is not required.
- (C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.

- (5)
- (A) If a matching agreement is disapproved by a Data Integrity Board, any party to such agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and Budget to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.
  - (B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that—
    - (i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;
    - (ii) there is adequate evidence that the matching agreement will be cost- effective; and
    - (iii) the matching program is in the public interest.
  - (C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).
  - (D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching program proposed by the inspector general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.
- (6) In the reports required by paragraphs (3)(D) and (6), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

**(v) Office of Management and Budget Responsibilities**



The Director of the Office of Management and Budget shall—

- (1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and
- (2) provide continuing assistance to and oversight of the implementation of this section by agencies.

The following section originally was part of the Privacy Act but was not codified; it may be found at § 552a (note).

Sec. 7(a) (1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.

- (3) the provisions of paragraph (1) of this subsection shall not apply with respect to--
  - (i) any disclosure which is required by Federal statute, or
  - (ii) any disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual; or
  - (iii) Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

The following sections originally were part of P.L. 100-503, the Computer Matching and Privacy Protection Act of 1988; they may be found at § 552a (note).

Sec. 6 Functions of the Director of the Office of Management and Budget.

- (iv) Implementation Guidance for Amendments -- The Director shall, pursuant to section 552a(v) of Title 5, United States Code, develop guidelines and regulations for the use of agencies in implementing the amendments made by this Act not later than 8 months after the date of enactment of this Act.

### **Sec. 9 Rules of Construction.**

Nothing in the amendments made by this Act shall be construed to authorize--

- (1) The establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies;
- (2) the direct linking of computerized systems of records maintained by Federal agencies;
- (3) the computer matching of records not otherwise authorized by law; or
- (4) the disclosure of records for computer matching except to a Federal, State, or local agency.

### **Sec. 10 Effective Dates.**

- (A) In General -- Except as provided in subsection (b), the amendments made by this Act shall take effect 9 months after the date of enactment of this Act.
- (B) Exceptions -- The amendment made by sections 3(b) [Notice of Matching Programs -- Report to Congress and the Office of Management and Budget], 6 [Functions of the Director of the Office of Management and Budget], 7 [Compilation of Rules and Notices], and 8 [Annual Report] of this Act shall take effect upon enactment.

## Appendix B

### A. Office of the Federal Register SORN Template – Full Notice

Agencies shall publish all system of records notices (SORNs) in the *Federal Register* using the appropriate format provided in the appendices to this Circular. Agencies shall use the language and section headings provided in the template and replace the language in brackets with the appropriate agency language.

Appendix II of A-108 provides the Office of the Federal Register SORN template for full notices that includes all of the required SORN elements. Agencies shall use this template when publishing a new SORN or choosing to publish a revised SORN in its entirety.

---

[Name of agency]

#### Privacy Act of 1974; System of Records

**AGENCY:** [Name of agency and, if applicable, agency component]. This caption should match the "Agency" and when appropriate, "Sub-agency" headings used at the top of the document. When a sub-agency and agency appear together, the sub-agency name is carried first and the agency name is represented by its commonly used acronym or other shortened expression. This caption may also identify a smaller organizational unit within the agency. (Examples: IRS, Treasury; or Departmental Offices, Treasury.)

**ACTION:** Notice of a [New/Modified] System of Records. This caption is designed to identify the type of document being presented; i.e., Notice of a Proposed System of Records; Final Rule, etc. It is not to describe or summarize the substance of a document.

---

**SUMMARY:** [A plain-language description of the system]. This caption explains the "why" and "what" of the document being issued. It is a brief description, written in language that a non-expert/member of the public will understand. It should allow the reader to determine the subject, the reason for the action, and the intended effect of the document. The text of this caption should not attempt to prove a point or argue a case.

**DATES:** [The deadline to submit comments on the proposal and the date on which any routine uses will be effective]. This caption presents the "when" of a document. It includes the dates within a document that are essential to the notice or rulemaking process (i.e., the deadline for receipt of public comments, the effective date of a notice or rule, or other dates relevant to public knowledge of the process).

For the purposes of the Privacy Act, a specific date must be specified in the notice or rule being published in the *Federal Register*. To alert the Office of the *Federal Register* to the need to compute the correct date(s), the following phrase may be used: "[insert date 30 days after publication in the *Federal Register*]."

Please note that the *Federal Register's* calculation of dates after publication will automatically bump a date forward if that date falls on a weekend or a Federal holiday. If the 30<sup>th</sup> day of publication in the *Federal Register* falls on a holiday on any day Monday through Thursday, the last day of publication is

moved to the next business day. If 30<sup>th</sup> day falls on Friday through Sunday, the last date is automatically jumped to the Monday following that weekend. It is standard so that the public will have a business day for a closing date. While weekend and holidays are counted within the period of days, the OFR will not let it fall on one unless it has specific instructions to do so.

**ADDRESSES:** [Instructions for submitting comments on the proposal, including an email address or a website where comments can be submitted electronically]. This caption explains the "where" of the document. It includes the address(es) where an individual may submit comments, attend a public hearing, or examine any relevant material in response to a proposed notice or rulemaking proceeding.

**FOR FURTHER INFORMATION CONTACT:** [Instructions for submitting general questions about the system]. Under this caption, the name and telephone number of a person within the agency who can answer questions about the notice or rulemaking should be included. Two or more persons may be listed as contacts regarding different aspects of a document.

**SUPPLEMENTARY INFORMATION:** [Background information about the proposal, including a description of any changes being made to the system and the purpose(s) of the changes]. Necessary information not identified by existing captions should be placed here. This caption should also contain any authority citation or other citation when appropriate. The text should be presented in language easily understood by the reader.

The cost of publishing the documents in the *Federal Register* is borne by the Treasury Office or Bureau submitting the documents. The "billing code" used by each component is maintained by Treasury Operations, Printing Services and is to be printed at the top right-hand corner of the first page of the preamble.

**FORMAT AND CONTENT OF THE NOTICE:** Since the notice is to assist an individual in determining if information on him/her might be in the system, the description of the categories should be clearly stated in non-technical terms which can be understood by people unfamiliar with data collection techniques. The notice contains certain prescribed data elements which are described below:

**IDENTIFICATION OF THE COMPONENT AND THE SYSTEM NUMBER:** The agency system identification number is assigned by the Treasury Department component establishing or altering the system of records. The system number follows the identification of the Treasury component responsible for the system (e.g., Treasury/DO .150).

**SYSTEM NAME AND NUMBER:** [A name for the system that is unambiguous and clearly identifies the purpose or character of the system, and the number of the system]. The system name should reflect the categories of individuals in the system and/or briefly describe the records in the system. The public should be able to determine from reading only the name whether the system covers Federal employees or the public; and, if it covers the public, what segment of the public is covered.

**SECURITY CLASSIFICATION:** [An indication of whether any information in the system is classified].

**SYSTEM LOCATION:** [The address of the agency and/or component responsible for the system, as well as the address of any third-party service provider]. The Department must specify each city/town and site where the system of records is located. However, exceptional situations may dictate not including the listing in the body of the notice; e.g., records kept in many locations such as regional and district offices nationwide. In these instances, it may be appropriate to publish a list as an appendix.

**SYSTEM MANAGER(S):** [The title, business address, and contact information of the agency official who is responsible for the system]. This section gives the title and business address of the agency official responsible, or officials if jointly responsible, for the system policies and practices outlined above. Personal names should not be included. Where locations are geographically dispersed (as in regional or district offices), the responsible official at each location should be listed in addition to the agency official responsible for the entire system. If the system does involve several managers and locations, they may be listed in an appendix. A contractor should not be designated as the system manager.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** [The specific authority that authorizes the maintenance of the records in the system].

**PURPOSE(S) OF THE SYSTEM:** [A description of the agency's purpose(s) for maintaining the system]. This element describes the objectives for collecting or maintaining information. The description should include all major purposes for which the records will be used by the agency.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** [The categories of individuals on whom records are maintained in the system]. The purpose of this requirement is to assist an individual in determining if information on him/her might be in the system. Therefore, the description of the categories should be clearly stated in non-technical terms understandable to people unfamiliar with data collection techniques.

**CATEGORIES OF RECORDS IN THE SYSTEM:** [The categories of records maintained in the system and, if practicable and useful for public notice, specific data elements]. The category of records should briefly describe, in non-technical terms, the types of information contained in the system. The additions of new categories of records not within the categories described in a current notice requires the issuance of a revised public notice before the change is put into effect.

**RECORD SOURCE CATEGORIES:** [The categories of sources of records in the system].

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** [Each routine use of the records contained in the system, including the categories of users and the purpose of such use]. The Act defines "routine use" as "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." Accordingly, this data element of the notice should identify the types of disclosures made from the system of records pursuant to 5 U.S.C. 552a (b)(3), the category of recipients, and the purpose of disclosure. The routine uses should be clearly and specifically stated so that they are understandable to the reader.

Disclosure to consumer reporting agencies: This element is included if information is to be disclosed to consumer reporting agencies to encourage repayment of an overdue debt pursuant to section 3 of the Debt Collection Act of 1982. If no such disclosure is to be made, this element should be omitted.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** [The policies and practices of the agency regarding the storage of records]. Storage: A description of the form in which the records are maintained (e.g., paper records, magnetic media).

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** [The policies and practices of the agency regarding retrieval of records]. The way in which the system is indexed and accessed (e.g., by name, identification numbers, combinations of personal

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** [The policies and practices of the agency regarding retention and disposal of records]. Retention and disposal: How long the records are maintained; if they are moved to a Federal Records Center or to the National Archives and Records Administration; if and how they are destroyed. A statement may be made to reference the records disposition schedule used.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** [A description of the administrative, technical, and physical safeguards to which the system is subject]. Safeguards: An explanation of measures taken to prevent unauthorized disclosure of records (e.g., physical security, personnel screening) and categories of individuals within the agency who have access.

**RECORD ACCESS PROCEDURES:** [The agency procedures whereby an individual can be notified at his or her request how he or she can gain access to any record pertaining to him or her in the system]. This describes the means by which individuals can find out how to gain access to records maintained about them. The agency official to contact should be provided or, if applicable, refer to "Notification Procedures." Any identifying information that individuals are required to provide for the agency to retrieve the necessary records should be given. Again, if applicable, a reference may be made to "Notification Procedures." Requesters should be advised to reasonably specify the record contents they seek. If the system is exempt from this provision, that fact should be stated.

**CONTESTING RECORD PROCEDURES:** [The agency procedures whereby an individual can be notified at his or her request how he or she can contest the content of any record pertaining to him or her in the system]. This section should describe the means by which individuals can contest a record. Requesters should be advised that they should reasonably identify the record and specify the information they are contesting and why they believe it is inaccurate, irrelevant, incomplete, untimely, or unnecessary. If the system is exempt from this provision, that fact should be stated.

**NOTIFICATION PROCEDURES:** [The agency procedures whereby an individual can be notified at his or her request if the system contains a record pertaining to him or her]. [The agency procedures whereby an individual can be notified at his or her request if the system contains a record pertaining to him or her]. The name of the agency office to which individuals should address their requests and the locations at which individuals may present a request to determine whether a system contains records pertaining to them. Include any identifying information that you require individuals to provide for the agency to ascertain whether a system contains a record about the individual. "Notification" is the "where and how" of determining if a Privacy Act system of records contains records pertaining to an individual. Where there are several locations for a single system of records, there may be a single system manager in charge of the entire system, and different personnel handling notification inquiries at each location. If the system involves several persons and locations, you may list them in an appendix. In order to avoid excessive delay and exchanges of correspondence, you should encourage individuals to request both notification and access at the same time.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** [Any Privacy Act exemptions promulgated for the system]: This identifies the subsections of the Act which permit the Department to exempt the system and the provisions of the Act from which the system is exempt. If the system is not to be exempt from provisions of the Act, this data element must be included with an indication of "None." See Chapter 10 for additional information pertaining to exemptions.

**HISTORY:** [Citation(s) to the last full *Federal Register* notice that includes all of the elements that are required to be in a SORN, as well as any subsequent notices of revision].

## **B. Office of the Federal Register SORN Template – Notice of Revision**

Agencies shall publish all system of records notices (SORNs) in the *Federal Register* using the format provided in the appendices to this Circular. Agencies shall use the language and section headings provided in the template and replace the language in brackets with the appropriate agency language.

Appendix III provides the Office of the Federal Register SORN template for revised notices that describe a modified system of records when the agency chooses not to publish the revised SORN in its entirety. The elements provided in the template are required to appear in any notice of a modified system of records. Elements omitted from the template shall be included in a notice of a modified system of records if there are revisions to those elements.

**[Name of agency]**

### **Privacy Act of 1974; System of Records**

**AGENCY:** [Name of agency and, if applicable, agency component].

**ACTION:** Notice of a Modified System of Records.

**SUMMARY:** [A plain-language description of the system].

**DATES:** [The deadline to submit comments on the proposal and the date on which any routine uses will be effective].

**ADDRESSES:** [Instructions for submitting comments on the proposal, including an email address or a website where comments can be submitted electronically].

**FOR FURTHER INFORMATION CONTACT:** [Instructions for submitting general questions about the system].

**SUPPLEMENTARY INFORMATION:** [Background information about the proposal, including a description of the changes being made to the system and the purpose(s) of the changes].

**SYSTEM NAME AND NUMBER:** [A name for the system that is unambiguous and clearly identifies the purpose or character of the system, and the number of the system].

**SECURITY CLASSIFICATION:** [An indication of whether any information in the system is classified].

**SYSTEM LOCATION:** [The address of the agency and/or component responsible for the system, as well as the address of any third-party service provider].

**SYSTEM MANAGER(S):** [The title, business address, and contact information of the agency official who is responsible for the system].

\*\*\*

[Agencies shall review the other elements in the full SORN template in Appendix II to this Circular and include elements for which revisions are necessary. For example, if an agency is modifying the categories of records in the system, the agency shall include that element in the notice of revision.]

\*\*\*

**HISTORY:** [Citation(s) to the last full *Federal Register* notice that includes all of the elements that are required to be in a SORN, as well as any subsequent notices of revision].

## C. Office of the Federal Register Notice of Rescindment Template

Agencies are required to publish a notice of rescindment in the *Federal Register* whenever they stop maintaining a previously established system of records. Agencies shall publish all notices of rescindment using the format provided in Appendix IV to this Circular. Agencies shall use the language and section headings provided in the template and replace the language in brackets with the appropriate agency language.

[Name of agency]

### Privacy Act of 1974; System of Records

**AGENCY:** [Name of agency and, if applicable, agency component].

**ACTION:** Rescindment of a System of Records Notice.

---

**SUMMARY:** [A plain-language description of the system that is being discontinued].

**DATES:** [The date on which the agency stopped or will stop maintaining the system of records].

**ADDRESSES:** [Instructions for submitting comments on the notice, including an email address or a website where comments can be submitted electronically].

**FOR FURTHER INFORMATION CONTACT:** [Instructions for submitting general questions about the discontinued system].

**SUPPLEMENTARY INFORMATION:** [Background information about the proposal, including an account of what will happen to the records that were previously maintained in the system and references to any other SORN that will pertain to the records].

**SYSTEM NAME AND NUMBER:** [The name and number of the system that is being discontinued].

**HISTORY:** [Citation(s) to the last full *Federal Register* notice that includes all of the elements that are required to be in a SORN, as well as any subsequent notices of revision].



## Appendix C

### A. Preamble

#### DEPARTMENT OF THE TREASURY

#### Privacy Act of 1974; System of Records

**AGENCY:** <Bureau>, Department of the Treasury.

**ACTION:** Notice of a <New/Modified> System of Records.

**SUMMARY:** In accordance with the Privacy Act of 1974, the Department of the Treasury (“Treasury” or the “Department”), <Bureau> proposes to <establish OR modify> a <new OR current> Treasury system of records titled, “Department of the Treasury, <Bureau> <SORN Number> - <System Name> System of Records.” <Include a plain language description of the system of record.>

**DATES:** Submit comments on or **before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The <new and/or significantly modified> routine uses will be applicable on **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

**ADDRESSES:** Comments may be submitted to the Federal eRulemaking Portal electronically at <http://www.regulations.gov>. Comments can also be sent to <Office Name>, <Bureau>, <Mailing Address>, Attention: Revisions to Privacy Act Systems of Records. Comments can be faxed to <(XXX) XXX-XXXX> or emailed to <email address>. For faxes and emails, please place “Revisions to SORN” in the subject line. Comments will be made available for public inspection upon written request or by making an appointment over the phone. The <Bureau> will make such comments available for public inspection and copying at the above listed location, on official business days between the hours of 9 a.m. and 5 p.m. Eastern Standard Time. Persons wishing to inspect the comments submitted must request an appointment by telephoning <(xxx) xxx-xxxx>. All comments received, including attachments and other supporting documents, are part of the public record and subject to public disclosure. All comments

received will be posted without change to www.regulations.gov, including any personal information provided. You should submit only information that you wish to make publicly available.

**FOR FURTHER INFORMATION CONTACT:** For general questions please contact: <Bureau Privacy Officer or Privacy Point of Contact Name, (Phone), Privacy Officer or Privacy Point of Contact, Bureau, and Address Information.> For privacy issues please contact: <Bureau Privacy Officer or Privacy Point of Contact Name, (Phone), Privacy Officer or Privacy Point of Contact, Bureau, and Address Information.>

### **SUPPLEMENTARY INFORMATION:**

In accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, the Department of the Treasury (“Treasury”), <Bureau> proposes to <establish OR modify> a <new OR current> Treasury system of records titled, “Department of the Treasury, <Bureau> <SORN Number> - <System Name> System of Records.”

<The information provided below should thoroughly outline the following in narrative form:

- Provide information about why the SORN is being published.
- Describe the purpose for which the Department is establishing the system of records.
- Provide the reader with the Bureau’s rationale for why we are collecting this information and what we are doing with it.
- Outline the subject authority (not general or housekeeping authorities).
- Identify whether the new system is required by a new rulemaking which is being published.
- If the SORN is being updated, please add **all changes** to the SORN since the last publication. Provide an explanation for changes to each section.
- Describe the effect of this proposed or updated system on individual’s privacy and outline steps the Department has taken to minimize the risk of unauthorized access to the system. (\*Do not merely say that the system has a minimal effect on privacy, cite the PIA/PCLIA and use the risks

assessed there to assist in crafting your answer).

- If the system of records is collecting information under the Paperwork Reduction Act using a form, include the OMB control number, expiration date, and title of the information collection.>

<Additionally, <Bureau> is issuing a Notice of Proposed Rulemaking, to exempt this system of records from certain provisions of the Privacy Act, elsewhere in the Federal Register.>

This <established OR modified> system will be included in Treasury's inventory of record systems.

Below is the description of the Treasury, <Bureau> <SORN Number> -<System Name> System of Records.

Treasury has provided a report of this system of records to the Committee on Oversight and Government Reform of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Office of Management and Budget (OMB), pursuant to 5 U.S.C. 552a(r) and OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act," dated December 23, 2016.

**NOTE:** *Within the system notice itself (below), do not rely on previously defined acronyms from the preamble; spell out everything anew and define the acronym again.*

**Dated:**

---

*Ryan Law,*

*Deputy Assistant Secretary for Privacy, Transparency, & Records.*