System of Records Notices

Official Guidance

The Privacy Office

System of Records Notices

The Privacy Office Official Guidance

Contents

Introduction

The Privacy Act of 1974, as amended, is one of the key legislative acts governing the protection of personally identifiable information (PII).[1] The Act, 5 U.S.C. § 552a, regulates the collection, maintenance, use, and dissemination of PII maintained by agencies and departments of the Executive Branch, including the Department of Homeland Security (DHS).[2]

The Privacy Act defines the requirements for Federal agencies in collecting and handling PII. The Privacy Act shapes the collection, use, maintenance, and dissemination of information about individuals that is stored and retrieved by personal identifier. It also gives individuals certain rights under specific circumstances to access and correct records about themselves.

Section 222(2) of the Homeland Security Act of 2002 specifically authorizes the Chief Privacy Officer to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with the fair information practices as set out in the Privacy Act of 1974."

This Guidance covers the requirements for identifying a system of records, the elements of a system of records notice (SORN), and the publication of a SORN. This Guidance briefly discusses exemptions to the Privacy Act as covered by Notices of Proposed Rulemakings (NPRMs) and Final Rules. This Guidance replaces the SORN guidance previously issued in February 2004 and augments, for DHS' purposes, guidance previously issued by the Office of Management and Budget, specifically *Privacy Act Implementation, Guidelines and Responsibilities*, July 9, 1975, and *Circular A-130* including *Appendix I*, November 28, 2000.

What is a SORN?

A SORN identifies the purpose for the system of records, which individuals are covered by information in the system of records, what categories of records are maintained about the individuals, and how the information is shared by the agency (routine uses).[3] The SORN also provides notice to the public regarding the rights and procedures of the Privacy Act for accessing and correcting PII maintained by an agency on an individual.[4]

The Privacy Act requires that a SORN be published in the *Federal Register* when PII is maintained by a Federal agency in a system of records and the information is retrieved by a personal identifier.[5]

---

[1] DHS' Privacy Impact Assessment Guidance uses the term personally identifiable information, or "PII." This Guidance will use the term "personally identifiable information" or "PII" except when referring to the retrievability requirement of the Privacy Act. In those cases the Guidance will use the term "personal identifier," as in, "information retrieved by personal identifier."

[2] Privacy Act of 1974 § 552(a), as amended.

[3] 5 U.S.C. § 552a(a)(5).

[4] 5 U.S.C. § 552a(a)(5).

[5] 5 U.S.C. § 552a(e)(4); 5 U.S.C. § 552a(5); *See*, Office of Management and Budget (OMB) *Circular A-130, Appendix I, § 4(c)*.

Principles

DHS is committed to analyzing and sharing information throughout the Federal, State, and local government so the urgent task of protecting the homeland can be carried out. At the same time, the Department must follow the requirements of the Privacy Act in its handling of PII.

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

Principle of Transparency - DHS must be transparent about what PII it collects, uses, disseminates, and maintains and provide individuals with notice of these applications.

Principle of Individual Participation - DHS must, to the extent practicable, collect information directly from the individual, as this practice increases the likelihood that the information will be accurate, and give notice to the individual at the time of collection of how the program provides for access, correction, and redress.

Principle of Purpose Specification - DHS must articulate with specificity the purpose of the program and tie the purpose(s) to the underlying mission of the organization and its enabling authority.

Principle of Data Minimization - DHS must ensure that PII is directly relevant and necessary to accomplish the specific purpose(s) of the program; this information should only be retained for as long as necessary and relevant to fulfill the specified purposes.

Principle of Use Limitation - DHS must use and share PII only for the purposes for which DHS collected the information and for which the individual received notice.

Principle of Data Quality and Integrity - DHS must ensure that PII is accurate, relevant, timely, and complete.

Principle of Security - DHS must use reasonable security safeguards to protect PII against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.

Principle of Accountability and Auditing - DHS must develop mechanisms to ensure compliance with these principles and with the program's other documentation such as any applicable Privacy Impact Assessment (PIA), SORN, and Privacy Threshold Analysis (PTA).

Requirements of the Privacy Act of 1974

A Privacy Act 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."[6]

In order to determine whether a system or program is required to publish a SORN, the program must answer affirmatively these three questions:

[6] 5 U.S.C. § 552a(a)(5).

- Does the system contain records as defined by the Privacy Act?
- Are the records in the system under the control of DHS?
- Are the records in the system retrieved by name or other identifying information (personal identifier)?[7]

Record

The Privacy Act defines a record as any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to:

- Name;
- Identifying number or identifier (e.g., social security number, employee number);
- Address;
- Medical history;
- Financial data; or
- Other identifying particular assigned to the individual, such as a finger or voice print, or a photograph.[8]

A Privacy Act record, by definition, contains PII. Do not confuse the Privacy Act definition of record with that of the Federal Records Act (44 U.S.C. Chapter 31) which applies to a larger set of Federal records regardless of whether they contain PII.

Control

In order for the Privacy Act to apply, the record must be under the control of DHS.[9] The purpose of the control requirement is to establish accountability for the provisions of the Privacy Act.[10] Records are under the control of DHS if they are maintained by or on behalf of the Department. Privacy Act Records stored by a contractor on behalf of DHS are regarded as controlled by DHS.

Retrieved by Personal Identifier

Finally, in order to be a system of records, the records that are under the control of DHS must be retrieved by name or other identifying information (personal identifier). A personal identifier might include an individual's name, address, e-mail address, telephone number, social security number, photograph, biometric information, or any other unique identifier that can be linked to an individual. This technical requirement means that DHS may have a set of records, but if the information is not retrieved by a personal identifier then the requirements mandated by the Privacy Act may not be applicable.

Mere collection of PII is not enough to trigger the SORN requirements of the Privacy Act, although it is enough to trigger a privacy impact assessment (PIA, see below). In order to trigger the SORN requirements of the Privacy Act information must actually be retrieved by personal identifier.

---

[7] 5 U.S.C. § 552a(a)(5); OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28952 (July 9, 1975).
[8] 5 U.S.C. § 552a(a)(4).
[9] OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28952 (July 9, 1975).
[10] *Id.*

As an example, assume that a DHS component operates a visitor management system. The system stores information about individuals by name and date of arrival at DHS, but the system retrieves information only by date of arrival at DHS. Under these circumstances the visitor management system is not a system of records under the Privacy Act. However, if the system were to retrieve information by an individual's identifying information, then it would qualify as a system of records under the Privacy Act.

Most information technology (IT) systems are designed to make record management and retrieval more efficient and less time consuming than a paper file system. In today's IT environment, most systems are designed to retrieve by multiple identifiers, including by personal identifier if required by the program.

It is important to note that once a system of records retrieves by personal identifier, the requirements of the Privacy Act apply regardless of whether the records are electronic or paper-based.

Individuals Covered by a SORN

The Privacy Act applies specifically to records under the control of an agency that holds PII about individuals who are U.S. Citizens (USC) and Lawful Permanent Residents (LPR). DHS policy extends the administrative protections contained in the Privacy Act to systems of records that have commingled PII on USCs, LPRs, and visitors (non-USCs and non-LPRs). These systems are referred to as "mixed-systems." Systems may be "mixed" if the system commingles data of USCs, LPRs, and visitors, or if there is a likelihood that an individual's status will change from visitor to USC or LPR during the retention period of the information. For more information on this policy, see the DHS Privacy Office Privacy Policy Guidance Memorandum 2007-1.[11]

The Privacy Act also applies to any PII controlled by DHS and maintained in a system of records, regardless of whether DHS maintains information in a classified system, if DHS handles information about government officials, or if the system is run by a contractor.

The Privacy Act does not apply to deceased persons or to corporations.

The Difference between SORN and PIA Requirements

A SORN is not a PIA. The E-Government Act of 2002 and Homeland Security Act of 2002 require DHS to conduct a PIA before developing or procuring IT systems or initiating projects that collect, maintain, or disseminate PII from or about members of the public, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of PII. In most cases a SORN and PIA will both be required when many IT systems which collect PII (requiring a PIA) can also retrieve by personal identifier (requiring a SORN); however in some cases only a PIA will be required.

The PIA should be initiated at the beginning of system development and issued alongside the SORN. The PIA informs the drafting of the SORN, but does not satisfy the requirements of the Privacy Act.[12]

If an existing collection of information with a completed PIA and SORN updates or changes its technology, even if the scope of the information collection remains the same,

[11] http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[12] See www.dhs.gov/privacy for information and guidance on PIAs conducted at DHS.

the PIA must be updated to analyze the new privacy impacts of the technology. The SORN covering the system must also be reviewed to ensure its continuing completeness and accuracy, but may not necessarily need to be updated.

Writing a SORN

The Privacy Act of 1974 requires agencies to publish a SORN in the *Federal Register* prior to the system of records becoming operational.[13] SORNs should be clear, unambiguous, and understandable to the general public, while fulfilling the necessary legal requirements of the Privacy Act.

DHS has developed a SORN template for Departmental consistency and ease of use. The template includes all required sections as well as the recommended language for certain sections of the SORN. Because DHS engages in a variety of operations, the SORN template is designed to apply to large variety of subject matter areas. The template is available on the Privacy Office website at www.dhs.gov/privacy.

All SORNs completed after the effective date of this guidance must be in conformance with the guidance contained herein and in the format provided in the template. All sections of the SORN template must be completed; please do not delete of modify sections of the template.

The following guidelines should be followed when drafting a SORN:

- *Remember the audience.* The SORN should be written in a manner that allows the public to understand the system of records being described.
- *Correct simple errors.* This document is meant to be published in the *Federal Register* and on DHS's website. Any SORN submitted to the Privacy Office should be free of spelling and grammatical errors.
- *Explain acronyms.* Spell out each acronym the first time it is used in the document. For example: Office of Management and Budget (OMB). Do not use acronyms in the summary of the notice.
- *Use plain English.* Use words, phrases, or names in the SORN that are readily known to the average person.
- *Define technical terms or references.* Keep in mind that readers may not understand technical terms when they are introduced without definition.
- *Cite legal references and other previously published documents.* Reference other programs and systems and provide explanations so that the general public can gain a complete understanding of the context of the program or system. If a document pertaining to the SORN has previously been published in the *Federal Register*, provide the citation, and if possible, a very brief description of the document type (e.g., system of records notice, statute, final or proposed rule).
- *Use the complete name of reference documents.* For example: National Institute of Science and Technology (NIST) *Special Publication 800-26, and Security Self-Assessment Guide for Information Technology Systems*. Subsequent references may use an abbreviated format.

[13] OMB Circular A-130, Appendix I, § 4(c).

Please ensure that the draft is employs the active rather than passive voice, whenever possible. Also, please use shorter and simpler sentences whenever possible to improve the clarity of the draft.

Contents of a SORN

The SORN template is provided with highlighted sections indicating where a component should add relevant information. The component is responsible for ensuring the accuracy of any language offered in the SORN template.

For every section before the Summary please follow the template.

Summary: This should be a concise summary of what the system does in layman's terms It should be no longer than three to four sentences. Please do not include abbreviations or citations to legal authority. For a legacy SORN, add legacy SORN title, *Federal Register* number and date issued (Month, Day, Year), areas reviewed and updated (e.g. categories of individuals, categories of records, routine uses), and exemptions from the Privacy Act.[14]

Dates: All SORNs, whether for new systems of records or updates to legacy systems of records, are required to be published in the *Federal Register* for a thirty (30) day public comment period prior to a system becoming operational. The following text is provided in the template:

For New Systems: *The established system of records will be effective [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]*.

Or:

For Existing Systems requiring an update or Legacy Systems that have not been re-issued under DHS: *Written comments must be submitted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]*.

Addresses: All SORNs will include the text provided below in the address section.

You may submit comments, identified by DHS-200X-XXXX by one of the following methods:

- *Federal e-Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.*
- *Fax: 1-866-466-5370.*
- *Mail: Hugo Teufel III, Chief Privacy Officer, Privacy Office, Department of Homeland Security, Washington, D.C. 20528.*
- *Instructions: All submissions received must include the agency name and docket number for this rulemaking. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.*
- *Docket: For access to the docket to read background documents or comments received go to http://www.regulations.gov.*

[14] A legacy SORN is any component SORN published prior to the creation of the Department of Homeland Security.

For Further Information: The component should add contact information for the individual in the component who can provide additional information on the SORN. Every SORN contains the following text provided in the template:

For general questions please contact: <component name and contact information>. For privacy issues please contact: Hugo Teufel III (703-235-0780), Chief Privacy Officer, Privacy Office, U.S. Department of Homeland Security, Washington, D.C. 20528.

Supplementary Information: The Supplementary Information section is divided into two (2) parts: Background and Privacy Act.

Background

This section should provide information addressing why DHS and the component are publishing the SORN. If a PIA is being conducted in conjunction with the SORN, much of the information from the overview and introduction of the PIA should be included in this section. In addition, this section needs to:

- Provide necessary background and reasons for which DHS is creating or modifying the system, including a description of any legacy systems, and the policy rationale for the creation or modification of the system of records.
- Identify whether Privacy Act exemption(s) are being taken and, if so, state that a NPRM is being published concurrently in the *Federal Register*.
- Provide a straightforward discussion of the routine uses if the records with common examples of the type of sharing envisioned under the routine use.

If the system of records is a legacy system of records, the background section must state:

Pursuant to the savings clause in the Homeland Security Act of 2002, Public Law 107-296, Section 1512, 116 Stat. 2310 (November. 25, 2002), the Department of Homeland Security (DHS) and its components and offices have relied on preexisting Privacy Act systems of records notices for the maintenance of records that concern <insert subject matter of legacy SORN>.

After discussing the system, following standard text must be included:

Consistent with DHS's information sharing mission, information stored in the <System Name> may be shared with other DHS components, as well as appropriate Federal, State, local, tribal, foreign, or international government agencies. This sharing will only take place after DHS determines that the receiving component or agency has a need to know the information to carry out national security, law enforcement, immigration, intelligence, or other functions consistent with the routine uses set forth in this system of records notice.

The conclusion of the Background section should repeat the information included in the Summary above.

Privacy Act

The Privacy Act embodies fair information principles in a statutory framework

governing the means by which the United States Government collects, maintains, uses, and disseminates personally identifiable information. The Privacy Act applies to information that is maintained in a "system of records." A "system of records" is a group of any records under the control of an agency for which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined to encompass United States citizens and legal permanent residents. As a matter of policy, DHS extends administrative Privacy Act protections to all individuals where systems of records maintain information on U.S. citizens, lawful permanent residents, and visitors. Individuals may request access to their own records that are maintained in a system of records in the possession or under the control of DHS by complying with DHS Privacy Act regulations, 6 CFR Part 5.

The Privacy Act requires each agency to publish in the Federal Register a description denoting the type and character of each system of records that the agency maintains, and the routine uses that are contained in each system in order to make agency record keeping practices transparent, to notify individuals regarding the uses to which personally identifiable information is put, and to assist individuals to more easily find such files within the agency. Below is the description of the "X" system of records.

The following text must be used to conclude the section:

In accordance with 5 U.S.C. 552a(r), DHS has provided a report of this new system/system change to the Office of Management and Budget and to Congress.

System of Records: This is the component and the system number as assigned by the Privacy Office. Most systems utilize the following naming scheme: DHS/COMPONENT-XXX. For example, a CBP system of records would be named DHS/CBP-XXX. Headquarters or Department-wide names generally follow this naming scheme: DHS/ALL-XXX.

System name: This is the name of the system of records. For example, Customs and Border Protection's Global Enrollment System would be "Customs and Border Protection, Global Enrollment System."

System classification: Please state whether the system is unclassified or classified. If the system is classified please state the level of classification (secret, top secret, etc.).

System location: For electronic or paper records, provide the location of the main servers or central file location as well as regional offices. Generally, it may be answered as "Offices of the Department of Homeland Security, Washington, D.C. 20528." If the information will be accessible from regional DHS offices or other ports of entry, then these locations should be noted as well.[15]

Categories of individuals covered by the system: List the types of individuals whose PII is contained in the system, e.g., DHS employees, contractors, individuals applying for benefits from the Department, or individuals seeking a grant from the Department. This

[15] OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28963 (July 9, 1975).

section needs to cover ALL individuals whose information will be in the system and will be retrieved by a personal identifier.

Please note, if you have a system that is operational and also maintains logs or audit trails with employee information, the employee information is likely covered by a separate employee information system of records notice.

Categories of records in the system: Describe all types of records in the system. For example, if the system or program collects full name, date of birth, social security number, or A-Number then each of those data elements should be listed individually in this section. If the system will maintain information from other systems, this should be noted in this section as well as in the Sources of Records section. The Categories of Records listed in this section should correspond to the records referenced in the Retrievability section below.

Authority for maintenance of the system: List the agency's authority to maintain the system. For example, if the Homeland Security Act requires your agency to perform a function which makes the creation of the system of records necessary, this section would read "the Homeland Security Act of 2002, Pub L. 107-296; 5 U.S.C. § 301." Do not list the Privacy Act in this section.[16]

Purpose(s): Describe the purpose of the system and explain why the program collects these particular records. This language may be culled from the system or program's PIA, if applicable.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

Routine uses apply to information sharing external to DHS. The term "routine use" is defined, with respect to the disclosure of a record, as "the use of such record for a purpose which is compatible with the purpose for which the record was collected." This section describes each situation in which DHS may share PII covered by this system of records notice pursuant to the Privacy Act § (a)(b)(3).

The routine uses must be compatible and consistent with the purpose for which the record was collected.[17] This ensures the public receives adequate notice of the Department's planned uses of the information in the system of records.

The following language must be included prior to the list of routine uses:

In addition to those disclosures generally permitted under 5 U.S.C. § 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside DHS as a routine use pursuant to 5 U.S.C. § 552a(b)(3) as follows:

Common routine uses for most system of records include sharing:

- For audits and oversight;
- For Congressional inquiries;
- To contractors, grantees, and experts to perform DHS authorized activities;
- For investigations of potential violations of law;

[16] OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28962 (July 9, 1975).
[17] OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28953 (July 9, 1975).

- For intelligence purposes;
- To the National Archives and Records Administration (NARA) for records management purposes;
- For litigation purposes; and
- For data breach and mitigation response.

The Appendix to this Guidance provides the DHS Library of Routine Uses that may be included in the SORN exactly as they are written. Routine uses must be compatible with the purpose of the original collection, so not all routine uses in the Library will be appropriate for a given SORN. DHS components must review each routine use carefully and determine which are appropriate and compatible for each particular system of records. Very few SORNs will need to use all the routine uses in the Library and some SORNs will have specific sharing needs that are not covered by these routine uses. Such systems and programs will need to develop additional routine uses to meet their needs. Further, the routine uses provided in the Library may be modified to meet specific mission needs, if sufficient justification is provided to the Privacy Office.

Routine uses apply to information sharing external to DHS. Information sharing within DHS does not need a specific routine use. DHS and its components are considered one agency; routine uses are not necessary to share information within DHS as long as the sharing is required for the performance of the recipient's official duties.[18] Information sharing within DHS should be addressed in the purpose and supplementary information to the SORN, and in a PIA when applicable.

Disclosure to consumer reporting agencies:

State what information is disclosed to consumer reporting agencies. If no information is disclosed, state 'None.'

Policies and practices for storing, retrieving, securing, retaining, and disposing of records in the system:

Storage:

Describe the manner in which the records are stored. For example, are the records hard copy or electronic? Are the records stored in a locked/unlocked metal file cabinet, and/or magnetic, optical, or electronic media? Many SORNs state that the records are stored in a central computer database. Also, if information is stored on backups in a different format, note that here.

Retrievability:

Describe the manner in which the records are identified for retrieval, such as by the name or other unique identifier associated with the individual. This includes unique identifiers assigned by the system itself. This section should correspond to the Categories of Records section above, for example, if a record will be retrieved by social security number, then social security number should be listed in the Categories of Records.

Safeguards:

[18] 5 U.S.C. § 552(a)(b)(1).

Describe the measures that are taken to ensure the records are not disclosed in an unauthorized manner, e.g., access limited to those with certain clearances, general nondisclosure obligations of employees, restrictions on transmittal of records from the system, electronic data encryption.[19]

With regard to the safeguard language provided in the template, if there are particular differences in a specific system of records safeguards which should be noted in addition to or in lieu of the provided text, or the provided text does not accurately describe the safeguards in place, the component should modify the text accordingly.

Retention and disposal:

Describe the retention and disposal schedule and provide the rationale for the period of time described. This should be done in conjunction with the component and DHS Records Manager. DHS and/or component records managers will ensure coordination and approval with the National Archives and Records Administration (NARA). If the system does not have a NARA approved retention schedule, the program must work with NARA and state that NARA approval is in development or pending. The component must consult with DHS Records Management and NARA prior to completion of the SORN.

System manager(s) and address:

Identify position title, and address of the system manager. This is generally the program manager that oversees the program.

Notification procedure:

List the basic information needed in order for the individual to make a proper information request of the system manager, and for the system manager to give a proper response to the request. [20]

Most SORNs will include the following language provided in the template or modify it with component specific information:

Individuals seeking notification of and access to any record contained in this system of records, or seeking to contest its content, may submit a request in writing to the component's FOIA Officer, whose contact information can be found at http://www.dhs.gov/foia under "contacts." If an individual believes more than one component maintains Privacy Act records concerning him or her the individual may submit the request to the Chief Privacy Officer, Department of Homeland Security, 245 Murray Drive, S.W., Building 410, STOP-0550, Washington, D.C. 20528.

When seeking records about yourself from this system of records or any other Departmental system of records your request must conform with the Privacy Act regulations set forth in 6 CFR Part 5. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty or perjury as a substitute for notarization. While no specific form is required, you may obtain forms for

[19] OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28966 (July 9, 1975).
[20] OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28961 (July 9, 1975).

this purpose form the Director, Disclosure and FOIA, http://www.dhs.gov or 1-866-431-0486. In addition you should provide the following:

- *An explanation of why you believe the Department would have information on you;*
- *Identify which component(s) of the Department you believe may have the information about you;*
- *Specify when you believe the records would have been created;*
- *Provide any other information that will help the FOIA staff determine which DHS component agency may have responsive records;*
- *If your request is seeking records pertaining to another living individual, you must include a statement from that individual certifying his or her agreement for you to access his or her records.*

Without this bulleted information the component(s) will not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

If this is a system that will be exempted from the access portions of the Privacy Act, then this section should include a statement justifying the exemptions claimed and the following:

Pursuant to 5 U.S.C. 552a(j) and (k), this system of records may not be accessed by members of the public for purposes of determining if the system contains a record pertaining to a particular individual. Nonetheless persons may seek access to records maintained in <System> as outlined in the Record Access Procedures section below. Requests for such access will be reviewed on a case-by-case basis.

Please note that in order to have an portions of a system of records exempted system under the Privacy Act, a Notice of Proposed Rulemaking and a Final Rule must first be issued.

Record access procedures:

This section describes how an individual gains access to his records.[21] This process will generally be the same as that stated in "Notification Procedures" and so the program may state:

See the 'Notification Procedure' above.

In some cases, a system may also mention the use of the DHS-wide redress program, Traveler Redress Inquiry Program (TRIP). In these cases, the following information should be included in the section:

If individuals are uncertain of which component of DHS handles the information, they may seek redress through the DHS Traveler Redress Program ("TRIP") (See 72 Fed. Reg. 2294, dated January 18, 2007). Individuals who, for example, believe they have been improperly denied entry, refused boarding for transportation, or identified for additional screening by a DHS component may submit a redress request through the TRIP. TRIP is a single point of contact for individuals who have inquiries or seek

[21] *See* OMB Circular A-130 §§ 7 (f) and (g). *See also*, OMB, *Privacy Act Implementation, Guidelines and Responsibilities*, 40 F.R. 28956 (July 9, 1975).

resolution regarding difficulties they experienced during their travel screening at transportation hubs such as airports and train stations or when crossing U.S. borders. Through TRIP, a traveler can correct erroneous information stored in DHS databases through one application. Redress requests should be sent to: DHS Traveler Redress Inquiry Program (TRIP), 601 South 12th Street, TSA-901, Arlington, VA 22202-4220 or online at www.dhs.gov/trip.

Contesting record procedures:

Describe how an individual contests information pertaining to that individual in the system of records. Similar to "Record Access Procedures", this section may be the same as "Notification Procedure." As such, the program may state, "See the "Notification Procedure" above."[22]

Record source categories:

Identify where DHS received the records, for example, from the individual applicant, other DHS systems of records, other Federal system of records, commercial data aggregators, or other commercial entities.

Systems exempted from certain provisions of the Privacy Act:

Often the response here is "None," because many systems do not meet the requirements to claim exemptions to the Privacy Act. If you believe an exemption applies to the system of records, please review the text of general exemptions (j) and specific exemptions (k) printed below. After reviewing the Privacy Act text determine which exemption is appropriate and consult with your component privacy officer, counsel, and the DHS Privacy Office to draft the NPRM.

Text of General Exemption (j) of the Privacy Act:

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

[22] *Id.*

individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.[23]

Text of Specific Exemptions (k) of the Privacy Act:

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.

[23] 5 U.S.C. § 552a(j)

> 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.[24]

Any exemptions taken in an NPRM must be published as a Final Rule before they are effective; simply publishing an NPRM will not exempt the system.[25]

SORN Development and Approval

- Prior to drafting a SORN, all components must contact the DHS Privacy Office to discuss appropriate routine uses for the system, and generally to coordinate DHS Privacy Act efforts. The DHS Privacy Office will be aware of similar initiatives in other components and will seek to reduce redundant work where possible and when in accordance with the Privacy Act.
- As an initial step, components of DHS are responsible for drafting SORNs, NPRMs, and Final Rules and ensuring their component privacy officer and counsel have approved the documents.
- The component then submits the draft documents to the DHS Privacy Office which reviews all DHS SORNs, NPRMs and Final Rules regardless of whether they originate from a component or headquarters.
- Once the DHS Privacy Office, component privacy officer, and component counsel have approved the document, the Office of General Counsel (OGC) at headquarters reviews all SORNs, NPRMs, and Final Rules.
- Once OGC approves the documents, the DHS Chief Privacy Officer signs all SORNs, NPRMs, and Final Rules.
- Upon approval of the document(s), the Privacy Office will send the required notices to Congress, OMB, and to the *Federal Register* for publication.[26]

Processing a SORN for Publication in the *Federal Register*

DHS will submit a SORN (and NPRM or Final Rule, if applicable) signed by the DHS Chief Privacy Officer to the Office of Management and Budget (OMB) who has 10 (ten) days to comment on the document(s).

- During its 10 day comment period OMB may provide comments. In such case DHS will hold publication until OMB's comments have been addressed.
- Upon clearance or lack of comment by OMB, DHS will publish the SORN for thirty (30) days before it is effective.

This means that OMB requires a SORN be submitted to OMB a minimum of forty (40) days prior to the system becoming operational.[27]

The publication requirements of the SORN are intended to:

---

[24] 5 U.S.C. § 552a(k).
[25] OMB Circular A-130, Appendix I, § 4(c)(5).
[26] OMB Circular A-130, Appendix I, §§ 4 (c) through (e) and § 5.
[27] OMB Circular A-130, Appendix I, § 4(c).

1) Prevent the creation of a system of records without first giving individuals an opportunity to review and comment on the purpose and routine uses for which their PII is collected; and

2) Help individuals locate systems of records that are likely to contain PII pertaining to them.

If you are publishing a SORN without an NPRM:

1) The system may be operational thirty (30) days after publication in the *Federal Register*.

If you are publishing a SORN with an NPRM:

1) The exemptions to the Privacy Act are not effective until the Final Rule has been published.

2) In order to effectuate the exemptions you must respond to any public comments solicited by the NPRM, and publish the responses in a Final Rule; and

3) Once the Final Rule is published, the exemptions are final and active.

Formatting:

- The following are formatting requirements of the *Federal Register*.[28]
- Left margin is 1.5 inches; all others are 1 inch.
- Times New Roman typeface in 12 point font.
- No right-justified margins.
- Double-space; 0 points advanced before and after the paragraph.
- No hyperlinks or superscripts; no hanging paragraphs.
- Headings are in bold; paragraphs are indented.
- The DHS SORN Template must be used to avoid any formatting problems.

[28] http://www.archives.gov/federal-register/write/handbook/.

Appendix

LIBRARY OF DHS SORN ROUTINE USES

LIBRARY OF DIFFERENT ROUTINE USES

CASE-SPECIFIC ROUTINE USES

Library of Different Routine Uses

AUDIT

- To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

BREACH MITIGATION AND NOTIFICATION

- To appropriate agencies, entities, and persons when (1) DHS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

CLEARANCE PROCESSING

- To an appropriate Federal, State, local, tribal, foreign, or international agency, if the information is relevant and necessary to a requesting agency's decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, or other benefit, or if the information is relevant and necessary to a DHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant or other benefit and when disclosure is appropriate to the proper performance of the official duties of the person making the request.

CONGRESSIONAL INQUIRIES

- To a Congressional office from the record of an individual in response to an inquiry from that Congressional office made at the request of the individual to whom the record pertains.

CONTRACTORS, et al.

- To contractors, grantees, experts, consultants, and the agents of thereof, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for DHS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to DHS officers and employees.

FORMER EMPLOYEES

- To a former employee of DHS, in accordance with applicable regulations, for purposes of responding to an official inquiry by a Federal, State, or local government entity or professional licensing authority; or facilitating communications with a former employee that may be necessary for personnel-related or other official purposes where the Department requires information or consultation assistance from the former employee regarding a matter within that person's former area of responsibility.

HEALTH

- To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations for the purpose of protecting the vital interests of a data subject or other persons, including to assist such agencies or organizations in preventing exposure to or transmission of a communicable or quarantinable disease or to combat other significant public health threats; appropriate notice will be provided of any identified health threat or risk.

INTELLIGENCE ACTIVITIES

- To a Federal, State, or local agency, or other appropriate entity or individual, or through established liaison channels to selected foreign governments, in order to provide intelligence, counterintelligence, or other information for the purposes of intelligence, counterintelligence, or antiterrorism activities authorized by U.S. law, Executive Order, or other applicable national security directive.

INTERNATIONAL AGREEMENTS

- To international and foreign governmental authorities in accordance with law and formal or informal international agreements.

INVESTIGATIONS, THIRD PARTIES

- To third parties during the course of a law enforcement investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the officer making the disclosure.

INVESTIGATIONS, OTHER AGENCIES

- To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations responsible for investigating or prosecuting the violations of, or for enforcing or implementing, a statute, rule, regulation, order, license, or treaty where DHS determines that the information would assist in the enforcement of civil or criminal laws.

LAW ENFORCEMENT INTELLIGENCE

- To a Federal, State, tribal, local or foreign government agency or organization, or international organization, lawfully engaged in collecting law enforcement intelligence information, whether civil or criminal, or charged with investigating, prosecuting, enforcing or implementing civil or criminal laws, related rules, regulations or orders, to enable these entities to carry out their law enforcement responsibilities, including the collection of law enforcement intelligence.

LAW ENFORCEMENT REFERRALS

- To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

LITIGATION, DOJ

- To the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) DHS or any component thereof, or (b) any employee of DHS in his/her official capacity, or (c) any employee of DHS in his/her individual capacity where DOJ or DHS has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and DHS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which DHS collected the records.

LITIGATION, OPPOSING COUNSEL

- To a court, magistrate, or administrative tribunal in the course of presenting evidence, including disclosures to opposing counsel or witnesses in the course of civil discovery, litigation, or settlement negotiations or in connection with criminal law proceedings or in response to a subpoena.

MATCHING PROGRAMS

- To other Federal agencies or non-Federal entities under approved computer matching efforts, limited to only those data elements considered relevant to determine eligibility under particular benefit programs administered by those agencies or entities or by DHS or any component thereof, to improve program integrity, and to collect debts and other monies owed under those programs.

NARA/RECORDS MANAGEMENT

- To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

REDRESS

- To a Federal, State, tribal, local, international, or foreign government agency or entity for the purpose of consulting with that agency or entity: (1) to assist in making a determination regarding redress for an individual in connection with the operations of a DHS component or program; (2) for the purpose of verifying the identity of an individual seeking redress in connection with the operations of a DHS component or program; or (3) for the purpose of verifying the accuracy of information submitted by an individual who has requested such redress on behalf of another individual.

SECURITY THREAT

- To Federal and foreign government intelligence or counterterrorism agencies when DHS reasonably believes there to be a threat or potential threat to national or international security for which the information may be useful in countering the threat or potential threat, when DHS reasonably believes such use is to assist in anti-terrorism efforts, and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

STATE DEPARTMENT

- To the Department of State in the processing of petitions or applications for benefits under the Immigration and Nationality Act, and all other immigration and nationality laws including treaties and reciprocal agreements.

TARGETED THREAT

- To an organization or individual in either the public or private sector, either foreign or domestic, where there is a reason to believe that the recipient is or could become the target of a particular terrorist activity or conspiracy, to the extent the information is relevant to the protection of life or property and disclosure is appropriate to the proper performance of the official duties of the person making the disclosure.

TESTING

- To appropriate Federal, State, local, tribal, or foreign governmental agencies or multilateral governmental organizations where DHS is aware of a need to utilize relevant data for purposes of testing new technology and systems designed to enhance national security or identify other violations of law.

Case-Specific Routine Uses

CIVIL RIGHTS ENFORCEMENT

- To the Department of Justice (DOJ), Civil Rights Division, for the purpose of responding to matters within the DOJ's jurisdiction to include allegations of fraud and/or nationality discrimination.

EMPLOYMENT ELIGIBILITY

- To an individual's prospective or current employer to the extent necessary to determine employment eligibility.

JUDGES AND REPRESENTATIVES

- To clerks and judges of courts exercising naturalization jurisdiction for the purpose of filing petitions for naturalization and to enable such courts to determine eligibility for naturalization or grounds for revocation of naturalization.

- To an attorney or representative (as defined in 8 CFR 1.1(j)) who is acting on behalf of an individual covered by this system of records in connection with any proceeding before USCIS or the Executive Office for Immigration Review.

MSPB & LABOR PROCEEDINGS

- To unions recognized as exclusive bargaining representatives under the Civil Service Reform Act of 1978, 5 U.S.C. 7111 and 7114, the Merit Systems Protection Board, arbitrators, the Federal Labor Relations Authority, and other parties responsible for the administration of the Federal labor-management program for the purpose of processing any corrective actions, or grievances, or conducting administrative hearings or appeals, or if needed in the performance of other authorized duties.

NEWS MEDIA

- To the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

OPM & PERSONNEL MATTERS

- To the United States Office of Personnel Management, the Merit Systems Protection Board, Federal Labor Relations Authority, or the Equal Employment Opportunity Commission when requested in the performance of their authorized duties.

EMPLOYEE SUITABILITY

- To any source or potential source from which information is requested in the course of an investigation concerning the retention of an employee or other personnel action (other than hiring), or the retention of a security clearance, contract, grant, license, or other benefit, to the extent necessary to identify the individual, inform the source of the nature and purpose of the investigation, and to identify the type of information requested.

- To designated officers and employees of Federal, State, local or international agencies in connection with the hiring or continued employment of an individual, the conduct of a suitability or security investigation of an individual, the grant, renewal, suspension, or revocation of a security clearance, or the certification of security clearances, to the extent that DHS determines the information is relevant and necessary to the hiring agency's decision.

GRIEVANCES

- To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee.

PAYROLL

- To the Department of Agriculture, National Finance Center (which provides payroll personnel processing services under a cross-servicing agreement) for purposes relating to the conversion of DHS employee payroll and personnel processing services to [new system name]; the issuance of paychecks to employees and distribution of wages; and the distribution of allotments and deductions to financial and other institutions, some through electronic funds transfer.

- To Federal, State, or local agencies for use in locating individuals and identifying their income sources to establish paternity, establish and modify orders of support, and for enforcement action

PROFESSIONAL MISCONDUCT

- To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

TAX AUTHORITIES, STATE AND LOCAL

- To the Internal Revenue Service and other jurisdictions which are authorized to tax the employee's compensation with wage and tax information in accordance with a withholding agreement with the Department of the Treasury pursuant to 5 U.S.C. §§ 5516, 5517, and 5520.

WAGE & SEPARATION

- To provide wage and separation information to another agency, such as the Department of Labor or Social Security Administration, as required by law for payroll purposes.

SOCIAL SECURITY ADMINISTRATION

- To the Social Security Administration (SSA) for the purpose of issuing a Social Security number and card to an alien who has made a request for a Social Security number as part of the immigration process and in accordance with any related agreements in effect between the SSA, DHS and the Department of State entered into pursuant to 20 CFR 422.103(b) (3); 422.103(c); and 422.106(a), or other relevant laws and regulations.