Privacy Impact Assessments

The Privacy Office Official Guidance

June 2010

Homeland Security

The Privacy Office
Department of Homeland Security
Washington, DC 20528
June 2010

Dear Colleagues,

The Privacy Impact Assessment is one of the most important instruments through which the Department creates transparency and establishes public trust in its operations. As the Chief Privacy Officer, I am responsible for ensuring that technologies developed and used by the Department sustain and do not erode privacy protections. As stewards of data on the citizens we serve, we all must strive to ensure privacy protection and awareness remain fundamental to the operations of the Department.

The PIA is a vital tool that evaluates possible privacy risks and the mitigation of those risks at the beginning of and throughout the development life cycle of a program or system. The transparency and analysis of privacy issues provided by a PIA demonstrates that the Department actively engages program managers and system owners on the mitigation of potential privacy risks. Privacy considerations must be contemplated systematically throughout the Department. By conducting PIAs, the Department demonstrates its examination of privacy during the development of programs and systems, thus upholding the Department's commitment to maintain public trust and accountability. By documenting the procedures and measures through which the Department protects the privacy of individuals, the Department is more transparent and can better carry out its mission.

Over the past several years, the Department of Homeland Security Privacy Office has issued guidance on Privacy Impact Assessments (PIA) to Departmental programs and systems. In 2004, the Privacy Office issued *Privacy Impact Assessments Made Simple*. In 2006 the Privacy Office issued *Privacy Impact Assessment Guidance 2006*. In 2007, the Privacy Office further refined its guidance and issued the *Privacy Impact Assessment Guidance 2007*.

The amended guidance presented here, *Privacy Impact Assessment Official Guidance 2010*, supersedes any previously

issued guidance. *Privacy Impact Assessment Official Guidance 2010* provides more streamlined guidance that reflects the requirements of both Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002, as well as updates based on the practices and policies of the Department.

We look forward to working together to establish and sustain privacy protections throughout the Department. Please contact my office at 703-235-0780 if you have any questions.

Respectfully,

Mary Ellen Callahan
Chief Privacy Officer
Chief Freedom of Information Act Officer
Department of Homeland Security

Contents

Introduction

Section 208 of the E-Government Act of 2002 requires all federal government agencies to conduct a Privacy Impact Assessment (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information (PII).

The PIA demonstrates to the public and to Congress that systems owners and developers have consciously incorporated privacy protections into the development, implementation, and operation of their systems. It is also a tool for individuals working on a program or accessing a system to understand how to best integrate privacy protections while working with PII.

Section 222 of the Homeland Security Act requires the Chief Privacy Officer of the Department to ensure that the technology used by the Department sustains privacy protections. The PIA is one mechanism through which the Chief Privacy Officer fulfills this statutory mandate. In addition, the Chief Privacy Officer is required to conduct PIAs for proposed rulemakings of the Department. The Chief Privacy Officer approves PIAs conducted by the Department's components.

This Guidance reflects the privacy requirements of both Section 208 of the E-Government Act of 2002 and Section 222 of the Homeland Security Act of 2002. The Chief Privacy Officer requires that all new PIAs follow this Guidance. The *Privacy Impact Assessment Guidance 2010* supersedes any previously issued Guidance.

What is a PIA?

A PIA is an analysis of how personally identifiable information is collected, used, disseminated, and maintained. It examines how the Department has incorporated privacy concerns throughout its development, design, and deployment of a technology, program, or rulemaking. "Personally identifiable

information" is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

The purpose of a PIA is to demonstrate that program managers and system owners have consciously incorporated privacy protections throughout the development life cycle of a system or program. This involves making certain that privacy protections are built into the system from the initiation of development, not after the fact when they can be far more costly or could affect the viability of the project.

The PIA process requires that candid and forthcoming communications occur between the program manager, system owner, the component's Privacy Officer, and the Privacy Office to ensure appropriate and timely handling of privacy concerns. Addressing privacy issues publicly through a PIA builds citizen trust in the operations of the Department of Homeland Security.

The PIA is a living document that needs to be updated regularly as the program and system are changed and updated, not just when the program or system is deployed. In cases where a legacy system is being updated, the PIA demonstrates that the system developers and program managers have implemented privacy protections into the updates.

A PIA should accomplish two goals: (1) it should determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form via an electronic information system; and (2) it should evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

By following this guidance, DHS fulfills the requirements for PIAs found in the E-Government Act and the Homeland Security Act.

Complying with the PIA Requirement

The Department of Homeland Security is committed to analyzing and sharing information through all of its agencies so that the urgent task of protecting the homeland can be carried out. At the same time, the Department must have in place robust protections for the privacy of any personally identifiable information that it collects, uses, disseminates, or maintains.

These protections seek to foster three concurrent objectives:

- Minimize intrusiveness into the lives of individuals;
- Maximize fairness in institutional decisions made about individuals; and
- Provide individuals with legitimate, enforceable expectations of confidentiality.

Federal law recognizes the ever-increasing amount of information stored in government systems and the speed with which computers can process and transfer data. Section 208 of the E-Government Act requires PIAs for all new or substantially changed technology that collects, uses, disseminates, or maintains personally identifiable information.

Section 222 of the Homeland Security Act provides the Chief Privacy Officer with broad authority to identify and comment on privacy matters resulting from proposed Departmental rules, regulations, and technologies and to do so in a public manner.

Subsection 1 of Section 222 acknowledges the Department's role in collecting personally identifiable information and includes a requirement that the Chief Privacy Officer of the Department ensure that technology used by the Department sustains and does not erode privacy protections.

Subsection 4 of Section 222 authorizes the Chief Privacy Officer to conduct a PIA of proposed Departmental rulemakings and regulations, which may or may not involve a particular technology. The authority under Subsection 4 is significant because a proposed rule may raise privacy

considerations regarding information practices that do not involve technology. This authority is separate and distinct from PIAs required under Section 208 of the E-Government Act.

The PIA is a document that helps the public understand what information the Department is collecting, why the information is being collected, how the information will be used and shared, how the information may be accessed, and how it will be securely stored. This document builds trust between the public and the Department by increasing transparency of the Department's systems and goals.

Information Covered by the PIA

A PIA should be completed for any program, system, technology, or rulemaking that involves personally identifiable information. Personally identifiable information is information in a program, system, online collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Examples of personally identifiable information include: name, date of birth, mailing address, telephone number, social security number, e-mail address, zip code, address, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), internet protocol addresses, biometric identifiers (fingerprints, e.g.), photographic facial images, any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify an individual.

Office of Management and Budget (OMB) Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, states that these data elements

may include a combination of gender, race, birth date, geographic indicator, and other descriptors.

In some cases the technology may only collect personally identifiable information for a moment. For example, a body screening device may capture the full scan of an individual. While the information may not be maintained for later use, the initial scan may raise privacy concerns and a PIA could be required. Examples of technology with privacy implications could include: systems utilizing radio frequency identification devices (RFID), biometric scans, data mining, or geospatial tracking.

In other cases, the technology may not be changing, but a program or system opts to use data from a new source such as a commercial aggregator of information. A PIA is required when such new sources of information are used.

"Private" Information

Personally identifiable information should not be confused with "private" information. Private information is information that an individual would prefer not be known to the public because it is of an intimate nature. Personally identifiable information is much broader; it is information that identifies a person or can be used in conjunction with other information to identify a person, regardless of whether a person would want it disclosed. If the information or collection of information connects to an individual it is classified as "personally identifiable information."

Example: A license plate number is personally identifiable information because it indirectly identifies an individual, but it is not deemed "private" because it is visible to the public. PIAs require analysis of the broader "personally identifiable information," not just the narrower "private information."

Privacy Act System of Records Notice (SORN) requirements v. PIA requirements

The Privacy Act of 1974 requires agencies to publish Systems of Records Notices (SORNs) in the *Federal Register* that describe the categories of records on individuals that they collect, use, maintain, and disseminate. Generally, the requirements to conduct a PIA are broader than the requirements for SORNs. The PIA requirement is triggered by the collection of personally identifiable information. SORNs are triggered by the collection of personally identifiable information that is actually *retrieved* by a personal identifier. Even if the collection of information remains the same and is already covered by an existing SORN or PIA, if the technology using the information is changed or updated, a PIA must be completed or updated to analyze the new impact of the technology. The SORN covering the system must also be reviewed to ensure its completeness and accuracy.

When to Conduct a PIA

Pursuant to Section 208 of the E-Government Act and Section 222 of the Homeland Security Act, a PIA should be conducted when a program or system is doing any of the following:

- Developing or procuring any new technologies or systems that handle or collect personally identifiable information. Conducting a PIA at the beginning of the development process allows the Privacy Office, program management, and system developers to ensure that the information is handled appropriately in the first instance. The PIA should show that privacy was considered from the beginning stage of system development. The PIA also provides for a framework to conduct ongoing reviews of these programs. The unique position of the Department in the federal landscape necessitates appropriate transparency of operations to garner public trust and approval.
- Developing system revisions. If an organization modifies an existing system, a PIA will be required. For example, if a program or system adds additional sharing of information

either with another agency or incorporates commercial data from an outside data aggregator, a PIA is required. Issuing a new or updated rulemaking that entails the collection of personally identifiable information. If an organization decides to collect new information or update its existing collections as part of a rulemaking, a PIA is required. The PIA should discuss how the management of these new collections ensures conformity with privacy law. Even if a component has specific legal authority to collect certain information or build a certain program or system, a PIA is required.

- Reviewing Information Collection Requests (ICR) including forms under the Paperwork Reduction Act (PRA). If the form or ICR is not covered by an existing PIA and SORN a new PIA will be required.

The PIA requirement does not provide an exemption for pilot testing a program or system. If a PIA is ultimately required for a system, any pilot of that system must have the PIA completed prior to the pilot launch. This applies even if the pilot initially plans to use anonymous data but will use personally identifiable information as it moves out of pilot. This is because the decisions affecting privacy are made leading up to the initiation of a pilot. Completion of a PIA prior to launch of a pilot ensures that privacy protections are considered during the development process instead of after a pilot has concluded when changes are potentially more costly and time-consuming.

Classified Information and Systems

A PIA should be conducted for all systems handling personally identifiable information including classified or law enforcement sensitive programs. Privacy Office personnel are cleared to read classified and sensitive materials. The Privacy Office will work cooperatively with the program manager and/or system owner to determine what information can be published.

Classified and sensitive systems conduct PIAs in order to ensure that the use and sharing of Department data has been carefully and thoughtfully considered.

Privacy Threshold Analysis

Some information systems will not require a full PIA. A program manager or system owner should submit a Privacy Threshold Analysis (PTA) to the component Privacy Office or Privacy Point of Contact (PPOC) for review to determine what privacy compliance documentation is required. If the component Privacy Office or PPOC does not have additional questions the PTA is submitted to the Privacy Office for review and approval. A properly completed and approved PTA provides documentation that a system owner assessed whether or not a full PIA is required.

PTAs are incorporated into the Certification & Accreditation (C & A) process, which is the process by which the Department assures its information technology systems meet appropriate security and operating standards. The Privacy Office reviews PTAs submitted by each system through the C & A process. The template of the PTA can be obtained from the Privacy Office or component Privacy Officers.

For example, you may submit a PTA on a system that collects no personally identifiable information. The system will have an official PTA on file documenting the determination that no PIA is required which allows the system to pass through C & A process.

PTAs are an effective tool for analyzing and documenting the potential privacy documentation requirements of other Departmental activities such as rules and forms. If a question exists regarding the need for a PIA or SORN, a PTA should be the first step of the analytical process.

Writing a PIA

Section 208 of the E-Government Act of 2002 requires agencies to make PIAs publicly available. PIAs should be clear, unambiguous, and understandable to the general public.

The length and breadth of a PIA will vary by the size and complexity of the program or system. Any new development that involves the processing of personally identifiable information should be able to demonstrate, through the PIA, that an in-depth analysis was conducted to ensure that privacy protections were built into the system.

A PIA Template has been developed for Departmental consistency and ease of use. The Template includes only the top level questions noted in the *Writing Guidance* section. The sublevel questions and examples in the outline below provide you with additional guidance in responding to the top level questions. The Template is available on the Privacy Office website at www.dhs.gov/privacy.

All PIAs completed after the effective date of this amended Guidance should be in the format outlined below. The Template is provided to eliminate inconsistency in Department PIAs and simplify the PIA process. All questions should be answered. If a particular question is not applicable please explain why it is not applicable.

The following drafting guidelines should be followed when drafting a PIA:

- *Remember the audience.* The PIA should be written in a manner that allows the public to understand the activities being described. The PIA should be written with sufficient detail to permit the Privacy Office to analyze the privacy risks and mitigation steps.
- *Correct simple errors.* This document is meant to be published on the Department's web site with portions possibly published in the *Federal Register*. Any PIA

submitted to the Privacy Office should be free of spelling and grammatical errors and written in active voice rather than passive voice.

- *Explain Acronyms.* Spell out each acronym the first time it is used in the document. For example: Office of Management and Budget (OMB).
- *Use Plain English.* Use words, phrases, or names in the PIA 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 first used.
- *Cite legal references and other previously published documents.* Reference other projects and systems and provide explanations, for the general public to gain a complete understanding of the context of the program or system. If a document has previously been published in the *Federal Register*, for example a system of records notice, 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.* National Institute of Science and Technology (NIST) SP 800-26, Security Self-Assessment Guide for Information Technology Systems. Subsequent references may use the abbreviated format. Full names for NIST documents can be found at NIST's website:

  http://csrc.nist.gov/publications/nistpubs.

Content of the Privacy Impact Assessment

Abstract

The abstract is the single paragraph that will be used to describe the program and the PIA. It will be published on the DHS web site and Federal Register. It should be a minimum of three sentences and a maximum of four, and conform to the following format:

- First sentence should include the name of the component and the system, technology, pilot, rule, program, or other collection (hereinafter referred to as "project"). Note: There are some instances where system is specifically called out.
- Second sentence should be a brief description of the project and its function.
- Third sentence should explain the reason the program is being created and why the PIA is required. This sentence should embody the same analysis that caused the project to be identified as a "privacy sensitive system" in the PTA, such as the project requires PII or the technology is privacy sensitive.

Overview

The overview creates the foundation for the entire PIA. The overview provides the context and background necessary to understand the project's purpose and mission and the justification for operating a privacy sensitive project. Include the following:

- Describe the purpose of the system, technology, pilot, rule, program, or other collection (hereinafter referred to as "project") the name of the Department Component(s) who own(s) or is funding the project, the authorizing legislation, and how it relates to the component's and Department's mission;
- Describe how the project collects and uses PII, including a typical transaction that details the life cycle from collection to disposal of the PII; and

- Describe the recommendation for how the program has taken steps to protect privacy and mitigate the risks described in the previous bullet. Note: Do not list every privacy risk in the succeeding analysis sections. Rather, provide a holistic view of the risks to privacy.

Additionally, consider the following as appropriate to the project:

- Describe the funding mechanism (contract, inter-agency agreement) that the project will operate under:
- Describe any routine information sharing conducted by the project both within DHS components and with external sharing partners and how such external sharing is compatible with the original collection of the information;
- Analyze the major potential privacy risks identified in the analysis sections of the PIA and discuss overall privacy impact of the program on individuals; and
- Identify the technology used and provide a brief description of how it collects information for the project.

Section 1.0
Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

List all statutory and regulatory authority for operating the project, including the authority to collect the information listed in question 2.1. Explain how the statutory and regulatory authority permits collection and use of the information. A simple citation without more information will not be sufficient for purposes of this document and will result in rejection of a Privacy Impact Assessment. You must explain how the statutory and regulatory authority permits the project and the

collection of the subject information. If the project collects Social Security numbers you must also identify the specific statutory authority allowing such collection.

If you are relying on another component and/or agency, please list their legal authorities.

Where information is received from a foreign government pursuant to an international agreement or memorandum of understanding, cite the agreement and where it can be found (i.e. website).

Example: Section 4011 of the Intelligence Reform and Terrorism Prevention Act of 2004, 49 U.S.C. § 44903(h)(4) (2004)..

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

For all collections of PII where the information is retrieved by a personal identifier, the Privacy Act requires that the agency publish a SORN in the *Federal Register*. Include the *Federal Register* citation for the SORN. If the information used in the project did not require a SORN, explain why not.

In some instances, an existing SORN (either program specific, DHS-wide, or Government-wide) may apply to the project's collection of information. In other instances, a new SORN may be required.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

Provide the date that the Authority to Operate (ATO) was granted or the date it is expected to be awarded. An operational system must comply with DHS Management Directive 4300A. Note that all systems containing PII are categorized at a minimum as "moderate" under Federal Information Processing Standards Publication 199. If the project does not trigger the C&A requirement, state that along with an explanation.

For a new project provide anticipated date of C&A completion.

If the project does not include technology, state that here.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

The project manager, in consultation with counsel and the component records management officer, must develop a records retention schedule for the records contained in the project that considers the minimum amount of time necessary to retain information while meeting the needs of the project. After the project manager and component records management officer finalize the schedule based on the needs of the project, it is proposed to NARA for official approval. Consult with your records management office for assistance with this question if necessary. If a NARA-approved schedule does not exist, explain what stage the project is in developing and submitting a records retention schedule.

Note: All projects may not require the creation of a new retention schedule.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

Section 2.0 Characterization of the information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the project collects, uses, disseminates, or maintains.

Identify (1) the categories of individuals for whom information is collected, and (2) for each category, list all information, including PII, that is collected and stored by the project.

This could include, but is not limited to: name, date of birth, mailing address, telephone number, social security number, e-mail address, zip code, facsimile number, mother's maiden name, medical record number, bank account number, health plan beneficiary number, any other account numbers, certificate/license number, vehicle identifier including license plate, marriage record, civil or criminal history information, medical records, device identifiers and serial numbers, education record, biometric identifiers, photographic facial image, or any other unique identifying number or characteristic.

If the project or system creates new information (for example, a score, analysis, or report) describe how this is done and the purpose of that information.

If the project receives information from another system, such as a response to a background check, describe the system from which the information originates, including what information is returned and how it is used.

2.2 What are the sources of the information and how is the information collected for the project?

A project may collect information directly from an individual, receive it via computer readable extract from another system, or create the information itself. List the individual(s) providing the specific information identified in 2.1.

If information is being collected from sources other than the individual, including other IT systems, systems of records, commercial data aggregators, and/or other Departments, state the source(s) and explain why information from sources other than the individual is required.

In some instances, DHS may collect information using different types of technologies such as radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why this information is used.

Commercial data includes information from data aggregators such as Choice Point or Lexis Nexis, where the information was originally collected by a private organization for non-governmental purposes, such as marketing or credit reporting.

Publicly available data includes information obtained from the internet, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator.

State whether the commercial or public source data is marked within the system.

Example: The commercial data is used as a primary source of information regarding the individual. Alternatively, the commercial data is used to verify information already provided by or about the individual.

2.4 Discuss how accuracy of the data is ensured.

Explain how the project checks the accuracy of the information.

Describe the process used for checking accuracy. If a commercial data aggregator is involved describe the levels of accuracy required by the contract. Sometimes information is assumed to be accurate, or in R&D, inaccurate information may not have an impact on the individual or the project. If the project does not check for accuracy, please explain why.

Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

Example: The project may check the information provided by the individual against any other source of information (within or outside your organization) before the project uses the information to make decisions about an individual.

2.5 Privacy Impact Analysis: Related to Characterization of the Information.

Given the specific data elements collected, discuss the privacy risks identified and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Consider the following Fair Information Practice Principles (FIPPs) below to assist in providing a response:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for DHS to ensure that personally identifiable information is accurate, complete, and current?

Section 3.0
Uses of the Information

The following questions require a clear description of the project's use of information.

3.1 Describe how and why the project uses the information.

List each use of the information collected or maintained. Provide a detailed response that states how and why the different data elements will be used. If Social Security numbers are collected, state why the SSN is necessary and how it was used.

Example: A project needs to collect name, date of birth, and passport information because that information provides the best matching capabilities against the terrorist screening database.

3.2 Does the project use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how DHS plans to use such results.

Many projects sift through large amounts of information in response to user inquiry or programmed functions. Projects may help identify areas that were previously not identifiable and need additional research by agents, analysts, or other employees. Some projects perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.

Discuss the results generated by the uses described in 3.1, including a background determination, link analysis, a score, or other analysis. These results may be generated electronically by the information system or manually through review by an analyst. Explain what will be done with the newly derived information.

Will the results be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

Example: The system will generate a response that there is a possible match to the terrorist screening database. This possible match will be maintained in the system with the information previously provided by the individual. A trained analyst will review the possible match and make a determination as to whether or not the individual is on the list. This determination will also be maintained in the system.

3.3 Are there other components with assigned roles and responsibilities within the system?

Discuss the intra-Departmental sharing of information (CBP to ICE). Identify and list the name(s) of any components or directorates within the Department with which the information is shared.

Example: Certain systems regularly share information because of the cross over of the missions of the different parts of DHS. For example, USCIS employees regularly use a CBP system to verify whether an individual has entered the country. USCIS employees note that the CBP system has been checked and the date on which it

was checked, but do not copy the information to the USCIS system.

3.4 Privacy Impact Analysis: Related to the Uses of Information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

Section 4.0 Notice

The following questions seek information about the project's notice to the individual about the information collected, the right to consent to uses of said information, and the right to decline to provide information.

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

In many cases, agencies provide written or oral notice before they collect information from individuals. That notice may include a posted privacy policy, a Privacy Act statement on forms, a PIA, or a SORN published in

the *Federal Register*. Describe what notice was provided to the individuals whose information is collected by this project. If notice was provided in the *Federal Register* provide the citation, (e.g. XX FR XXXX, Date).

If notice was provided in a Privacy Act statement, attach a copy of the notice for review. Describe how the notice provided for the collection of information is adequate to inform those impacted.

Consult your privacy office and legal counsel on issues concerning the notice to the public for an information collection such as a form.

If notice was not provided, explain why. For certain law enforcement projects, notice may not be appropriate – this section of the PIA would then explain how providing direct notice to the individual at the time of collection would undermine the law enforcement mission.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

This question is directed at whether the individual from or about whom information is collected can decline to provide the information and if so, whether the consequences of providing the information are included in the notice.

Additionally, state whether an individual may provide consent for specific uses or whether consent is given to cover all uses (current or potential) of his/her information. If specific consent is permitted or required, how does the individual consent to each use?

If notice is provided to explain how an individual may exercise the right to consent to particular uses or decline to provide information describe the process. If this is not an option, explain why not. In some cases,

declining to provide information simply means the individual chooses not to participate in the project.

4.3 Privacy Impact Analysis: Related to Notice.

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

Principle of Individual Participation: Has the program provided notice to the individual of how the program provides for redress including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?

Section 5.0
Data Retention by the project

The following questions are intended to outline how long the project retains the information after the initial collection.

5.1 Explain how long and for what reason the information is retained.

The purpose of this question is to identify the specific types of information the project retains. Is all the information the project collects retained? Is there a specific sub set of information retained?

Example: A project may collect extensive PII initially for the purpose of verifying the identity of an individual for a background check. Upon completion of the background check, the project will maintain the new information, the results of the background check (approved/not approved) and delete all application information.

This section should explain the nexus between the original purpose for the collection and this retention period. The minimum amount of information should be maintained for the minimum amount of time in order to support the project.

Example: The project retains the information for the period of time in which fraud could be prosecuted and then the information is deleted.

In some cases, DHS may choose to retain files in active status and archive them after a certain period of time. State active file retention periods as well as archived records, in number of years, as well as the approved or proposed NARA records schedule. Discuss when the time periods begin for inputs, outputs, and master files. Project managers should work with component records officers early in the development process to ensure that appropriate retention and destruction schedules are implemented.

5.2 Privacy Impact Analysis: Related to Retention.

Discuss the risks associated with the length of time data is retained. How were those risks mitigated?

Although establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the project information sharing external to the Department. External sharing encompasses sharing with other federal, state and local government, and private sector entities

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Discuss the external Departmental sharing of information (for example, CBP to FBI). Identify the name or names of the federal agencies and foreign governments.

Example: Customs and Border Protection may share biographic information on an individual with the Federal Bureau of Investigation in order for FBI to conduct a background check. Alternatively, USVISIT may share biographic and biometric information with the intelligence community in order to identify possible terrorists.

For state or local government agencies, or private sector organizations list the general types rather than the specific names.

Example: The program shares information with state fusion centers that have a posted privacy policy. In particular, discuss any international agreements that require information sharing as part of normal agency operations

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Note which routine uses support the sharing described in 6.1 related to normal business operations.

Example: Routine use H allows DHS to share biographic information with the FBI to conduct a background check. This is compatible with the original collection because the Immigration and Naturalization Act (INA) requires that USCIS determine whether an individual has committed any disqualifying crimes. Without checking with the FBI, DHS would be unable to meet this requirement of the law.

6.3 Does the project place limitation on re-dissemination?

Describe any limitations that may be placed on external agencies further sharing the information provided by DHS. In some instances, the external agency may have a duty to share the information, for example through the information sharing environment. But, before

disclosing the information to the individual the external agency is required to verify with DHS.

6.4 Describe how the project maintains a record of any disclosures outside the Department?

Under subsection (c) of the Privacy Act, DHS must retain an accounting of what records were disclosed to whom, even for systems that are otherwise exempt from certain provisions of the Act. A project may keep a paper or electronic record of the date, nature, and purpose of each disclosure, and name and address of the individual or agency to whom the disclosure is made. If the project keeps a record, list what information is retained as part of the accounting requirement. A separate system does not need to be created to meet the accounting requirement, but the program must be able to recreate the information noted above to demonstrate compliance. If the project does not, explain why not.

6.5 Privacy Impact Analysis" Related to Information Sharing?

Discuss the privacy risks associated with the sharing of information outside of the Department. How were those risks mitigated?

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

Section 7.0
Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

7.1 What are the procedures that allow individuals access to their information?

Describe any procedures or regulations your component has in place that allow access to information collected by the system or project and/or to an accounting of disclosures of that information. Generally speaking, these procedures should include the Department's FOIA/Privacy Act practices. If the Privacy Act does not apply, state why this is the case. If additional mechanisms exist, include those in this section. For example, if your component has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the Department's procedures.

If the system is exempt from the access provisions of the Privacy Act, explain the basis for the exemption and cite the Final Rule published in the Code of Federal Regulations (CFR) that explains this exemption. If the project is not a Privacy Act system, explain what procedures and/or regulations are in place that cover an individual gaining access to his/her own information.

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Discuss the procedures for individuals to address possibly inaccurate or erroneous information. If the correction procedures are the same as those given in

question 7.1, state as much. If the system has exempted itself from the provisions of the Privacy Act, explain why individuals may not access their records.

7.3 How does the project notify individuals about the procedures for correcting their information?

Individuals may be made aware of redress procedures through the notices described above in Section 4 or through some other mechanism. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are weakened significantly.

Example: Some programs provide the information related to redress in a letter when an individual is given an initial negative determination regarding receiving a particular benefit. This would give the individual clear notice of how to address possible problems with the information the Department holds on him. Other programs depend upon a notice in the workplace rather than direct notice to the individual, so redress may be more difficult for the individual.

7.4 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Example: If a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

Section 8.0
Auditing and Accountability

The following questions are intended to describe technical and policy based safeguards and security measures.

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

Auditing measures are recommended and should be discussed, but other possible technical and policy safeguards such as information sharing protocols, special access restrictions, and other controls should be discussed here as well.

Do the audit measures discussed above include the ability to identify specific records each user can access? Describe the different roles in general terms that have been created to provide access to the project information. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Explain whether the project conducts self audits, third party audits, reviews by the Office of Inspector General or Government Accountability Office (GAO).

Does the IT system have automated tools to indicate when information is possibly being misused?

Example: If certain celebrity records are accessed, a supervisor is notified and reviews to ensure that the records were properly used.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

DHS offers privacy and security training. Each project may offer training specific to the project, which touches on information handling procedures and sensitivity of information. Discuss how individuals who have access to PII are trained to appropriately handle it.

Explain what controls are in place to ensure that users of the system have completed training relevant to the project.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Describe the process and authorization by which an individual receives access to the information held by the project, both electronic and paper based records. Identify users from other agencies who may have access to the project information and under what roles these individuals have such access. Describe the different roles in general terms that have been created that permit access to such project information.

Specifically, if remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication).

Example: Certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

8.4 How does the project review and approve information sharing requirements, MOUs, new uses of the information, new access to the system by organizations within DHS and outside?

Example: All MOUs are reviewed by the program manager, component Privacy Officer, and counsel and then sent to DHS for formal review.

Approval and Signature Page

Provide a contact name and number for the privacy officer or program manager of the program covered by this PIA, as well as a place for the Chief Privacy Officer to sign the final PIA when it is completed and approved.

Contact Us.

Privacy Office

U.S. Department of Homeland Security
Washington, DC 20528

Email: PIA@dhs.gov
Phone: 703-235-0780
Website Link: www.dhs.gov/privacy

Privacy Office

Mary Ellen Callahan
Chief Privacy Officer

John Kropf
Deputy Chief Privacy Officer

Privacy Compliance Staff

Rebecca Richards
Director, Privacy Compliance

Eric Leckey
Associate Director, Privacy Compliance

Jamie Pressman
Associate Director, Privacy Compliance

Tamara Baker
Privacy Analyst

Christal Hoo
Privacy Analyst

Shannon Kelso
Privacy Analyst

Erin Odom
Administrative Assistant

Component Privacy Officers

Laurence Castelli
Customs and Border Protection

Paul Hasson
US-VISIT

Donald Hawkins
United States Citizenship and Immigration Services

Thomas McQuillan
Federal Emergency Management Agency

Latita Payne
United States Secret Service

Peter Pietra
Transportation and Security Administration

Lyn Rahilly
Immigration and Customs Enforcement

Sherry Richardson
United States Coast Guard

Privacy Office

U.S. Department of Homeland Security
Washington, DC 20528
703-235-0780
www.dhs.gov/privacy
Email: PIA@dhs.gov