Privacy Impact Assessments

Official Guidance

The Privacy Office

May, 2007

Dear Colleagues,

The Privacy Impact Assessment (PIA) is one of the most important instruments through which the Department 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. 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.

By conducting a PIA, the Department demonstrates its consideration of privacy during the development of programs and systems and thus upholds the Department's commitment to maintain public trust and accountability. Without the trust of the public, the Department's mission is made more difficult. By documenting the procedures and measures through which the Department protects the privacy of individuals, the Department can better carry out its mission.

Over the past several years, the Department of Homeland Security Privacy Office has issued guidance on PIAs 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. The amended guidance presented here, *Privacy Impact Assessment Guidance* 2007, supersedes any previously issued guidance. *Privacy Impact Assessment Guidance* 2007 reflects the requirements of both Section 208 of the E-Government Act of 2002 and the Section 222 of the Homeland Security Act of 2002, as well as updates based on the practices and policies of the Department.

Respectfully,

Hugo Teufel III
Chief Privacy Officer,
Chief Freedom of Information Act Officer
The Privacy Office
United States Department of Homeland Security

Privacy Impact Assessments

The Privacy Office Official Guidance

Contents

Introduction

Section 208 of the E-Government Act of 2002 requires all federal government agencies to conduct PIAs for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information.

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 the Department's proposed rulemakings. 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* 2007 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 the development, design, and deployment of a technology 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 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 or 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.

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 should 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 ensures 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 document by which the Department memorializes its compliance with the E-Government Act of 2002 and Homeland Security Act of 2002 is called a "Privacy Impact Assessment," or "PIA." A PIA analyzes how personally identifiable information is collected, used, stored, and protected by the Department and examines how the Department has incorporated privacy concerns throughout its development, design, and deployment of a technology or rulemaking.

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.

The PIA demonstrates that the Department considers privacy from the beginning stages of program and system development and throughout the life cycle of the program or system. The PIA process and the document itself are intended to ensure that privacy protections are built into the program or system from the start, not after the fact when privacy concerns can be far more costly to address or could affect the investment's viability. Additionally, the PIA demonstrates that the program and system owners have made technology choices that reflect the incorporation of privacy into the system's architecture. In order to make the PIA comprehensive and meaningful, it should involve collaboration between program or system owners and information technology, security, and privacy experts.

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 personally identifiable information 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 the requirements for PIAs found in the E-Government Act and the Homeland Security Act will be fulfilled.

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 Department employee or contractor.

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 (e.g., fingerprints), 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.

Regarding "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."

Regarding 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. SORN requirements 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

Per Section 222 of the Homeland Security Act and Section 208 of the E-Government 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. A PIA is required for all budget submissions to OMB. The PIA should show that privacy was considered from the beginning stage of system development. If a program or system is beginning with a pilot test, a PIA is required prior to the commencement of the pilot test.
- 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. Appendix I of this document provides extensive examples.
- 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.

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 and Sensitive Information and Systems

A PIA should be conducted for all systems handling personally identifiable information, including classified or sensitive systems, but the program or system may be exempted from the requirement to publish the PIA. Note that Privacy Office personnel are cleared to read classified and sensitive materials, and prior to public release of any PIA all proper redactions will be made. The Privacy Office will work cooperatively with the program manager or system owner to make all appropriate redactions or determine whether the PIA is exempt from the publication requirement.

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

Privacy Threshold Analysis

Some information systems will not require a full PIA. A program manager or system owner can complete and submit to the Privacy Office a Privacy Threshold Analysis (PTA) to aid determining whether a full PIA is required. A properly completed and approved PTA provides documentation that a system owner assessed whether or not a full PIA is required.

For any program or system within the Department, a PTA should be conducted in order to determine if a full PIA is necessary. To this end, 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.

In addition to the use of PTAs in the C & A process, PTAs have proven to be an effective tool for analyzing and documenting the potential privacy documentation requirements of Departmental activities. 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 this guidance 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. All questions should be answered. If a particular question is not applicable please explain why it is not applicable.

The following 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.
- *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 programs 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 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 such as National Institute of Science and Technology (NIST) Special Publication 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.

Remember to utilize such writing techniques as the use of consistent terms and the use of active voice rather than passive voice. The use of shorter and simpler sentences will improve the clarity of the document.

Lastly, the PIA template is provided to eliminate inconsistency in Department PIAs and to simplify the PIA process. Because the Department engages in a myriad of operations, the PIA template is designed to encompass a large variety of subject matter areas. If a particular question is not applicable to your program or system please state that it is not applicable and explain why it is not applicable. Simply leaving a response as "not applicable" without an explanation is not acceptable.

Content of the Privacy Impact Assessment

Abstract

This brief paragraph will be the explanatory paragraph used for publication purposes. The abstract should be a minimum of three sentences and a maximum of four, if necessary. It should conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

The following are examples of why the PIA is being conducted: Component X conducted this PIA because the system collects personally identifiable information; this PIA serves as an update to the PIA published on January 1, 20XX; this PIA is being conducted to assess the privacy impact of the new technology being deployed by the Department.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses to questions asked in the PIA.

The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted by the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems and their functions, where relevant; and,
- A citation to the legal authority to operate the program or system.

Section 1.0
Characterization of the Information

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

rule, or technology being developed.

1.1 What information is collected, used, disseminated, or maintained in the system?

1.1.1 Identify and list all personally identifiable information that is collected and stored in the system. 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, device identifiers and serial numbers, uniform resource locators (URLs), education record, internet protocol addresses, biometric identifiers, photographic facial image, or any other unique identifying number or characteristic.

1.1.2 If the system creates information (for example, a score, analysis, or report) please list the information the system is responsible for creating.

1.1.3 If the system receives information from another system, such as a response to a background check, describe what information is returned to the system.

1.2 What are the sources of the information?

1.2.1 List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

1.2.2 Describe why information from sources other than the individual are required. For example, if a program or system is using data from a commercial aggregator of information or data taken from public websites, state the fact that this is where the information is coming from and then in 1.3 indicate why the program or system is using this source of data.

1.2.3 If the system creates information (for example, a score, analysis, or report) please list the system as a source of information.

1.3 Why is the information being collected, used, disseminated, or maintained?

1.3.1 Please include a statement of why the particular personally identifiable information that is collected and stored in the system is necessary to the component's or Department's mission. Merely stating the general purpose of the system without explaining why particular types of personally identifiable information should be collected and stored is not an adequate response to this question.

1.3.2 For example, a statement that a system may collect name, date of birth and biometrics in order to verify an individual's identity at the border is adequately specific. However, stating that the above information will be collected to ensure border security is not sufficient. Similarly, it would be more appropriate to state, for example, that information is collected to compare to the terrorist watch lists then to say it is generally used to secure airline flights.

1.3.3 If the system collects, uses, disseminates, or maintains commercial data please include a discussion of why commercial data is relevant and necessary to the system's purpose.

1.4 How is the information collected?

1.4.1 This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies such as radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices, or other technology used in the storage or transmission of personally identifiable information?

1.4.2 If the information is collected on a form and is subject to the Paperwork Reduction Act, please give the form's OMB control number and the agency form number.

1.5 How will the information be checked for accuracy?

1.5.1 Explain whether information in the system is checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual. If not, explain whether your organization has any other rules or procedures in place to reduce the instances in which inaccurate data is stored in the system.

1.5.2 If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

1.6 What specific legal authorities, arrangements, and/or agreements defined the collection of information?

1.6.1 Please list the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Please provide the authorities in a manner understandable to any potential reader, i.e., please do not simply provide a legal citation; please use statute names or regulations in addition to citations.

1.7 Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

1.7.1 For example, if the program manager or system owner chose to restrict collection of information please include the reasons behind the decreased scope of collection. Further, if specific risks are inherent to the sources or methods of collection, please discuss how those risks were mitigated.

1.7.2 The analysis should sufficiently explain how the collection serves the purpose(s) of the program or system and the mission of the organization. The information collected should be relevant and necessary to accomplish the stated purpose(s) and mission. The information also should be collected only through legal and fair means.

1.7.3 Please identify how any risks associated with the sources of information have been mitigated, e.g., information is collected directly from the individual, or information not directly collected is verified or corroborated to increase accuracy.

Section 2.0
Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe all uses of the information.

2.1.1 Identify and list each use (internal and external to the Department) of the information collected or maintained.

2.2 What types of tools are used to analyze the data and what type of data may be produced?

2.2.1 Many systems sift through large amounts of information in response to user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Please discuss any type of analysis the system conducts and the data that is created from the analysis.

2.2.2 If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it 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.

2.2.3 This question may be related to questions 1.1 and 1.2 which, among other things, are intended to capture information created by the system.

2.3 If the system uses commercial or publicly available data please explain why and how it is used.

2.3.1 This response should explain the following:

2.3.1.1 If commercial data or publicly available data (open source) is directly or indirectly used, discuss those uses in this section.

2.3.1.2 If a program, system, or individual analyst uses commercial data or publicly available data please discuss it here.

2.3.1.3 If commerical data or publicly available data is used to verify information already maintained by DHS, please discuss.

2.3.1.4 If new information previously not maintained by DHS is brought from an outside source, whether commericial or not, please discuss here.

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

2.4.1 For example, is appropriate use of information covered in training for all users of system? Are disciplinary programs or system controls (i.e. denial of access) in place if an individual is found to be inappropriately using the information?

2.4.2 If a system performs analytical functions or relies on commercial data in any way, discuss how data accuracy and integrity are preserved. If the system is creating new information, how is the information used and deemed to be reliable?

2.4.3 If commercial data is used, how is the reliability of the data assessed with regard to its value to the purpose of the system?

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 How long is information retained?

3.1.1 In some cases DHS may choose to retain files in active status and archive them after a certain period of time. Please state active file retention periods as well as archived records, in number of years, as well as the General Records Schedule. Component Records Officers should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

3.2.1 The component records management officer should provide a proposed schedule for the records contained in your system. After the component Records Officer provides a proposed schedule, the schedule should be formally offered to NARA for official approval.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

3.3.1 Although establishing retention periods for records is a formal process, there are policy considerations behind how long a system keeps information. The longer a system 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 Federal Records Act and NARA and the schedule should align with the stated purpose and mission of the system.

Section 4.0
Internal Sharing and Disclosure

The following questions are intended to describe the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

4.1.1 The term "internal" references directorates, components, offices, and any other organization within the Department. This question is directed at the intra-Departmental sharing of information.

4.1.2 Identify and list the name(s) of any directorates, components, offices, and any other organizations within the Department with which the information is shared.

4.1.3 If you have specific authority to share the information, please provide a citation to the authority.

4.1.4 For each interface with a system outside your Directorate, component, or office, state what specific information is shared with the specific components, agencies, and any other organizations within the Department.

4.2 How is the information transmitted or disclosed?

4.2.1 Describe how the information is transmitted to each Directorate, component, or office and any other organization within the Department. For example is the information transmitted electronically, by paper, or by some other means?

4.2.2 Is the information shared in bulk, on a case by case basis, or does the sharing partner have direct access to the information?

4.2.3 If specific measures have been taken to meet the requirements of OMB Memorandums M-06-15 and M-06-16, please note them here.

4.3 Privacy Impact Analysis: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

4.3.1 For example, if another Departmental Directorate, component, or office has access to the system that your Directorate controls, discuss how access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing of information.

4.3.2 Also, please discuss how the uses of the information are in accord with the stated purpose and use of the original collection, potential risks, mitigiation of risks, and compliance with legal authority.

Section 5.0
External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to the Department which includes Federal, state and local government, and the private sector.

5.1 With which external organization(s) is the information shared, what information is shared, and for what purpose?

5.1.1 The term "external" references other departments, agencies and organizations that are not a part of the Department of Homeland Security. This could be other departments, law enforcement and intelligence agencies, the private sector, and state and local entities. This question is directed at inter-departmental sharing, as well as with private entity and state or local information sharing.

5.1.2 Identify and list the name or names of the federal, state, or local government agency or private sector organization with which the information is shared.

5.1.3 If a SORN has been published for the system, please summarize the most relevant routine uses. For example, if the system provides full access to another agency for their use of the information, please include it in the summary. An example of a less relevant routine use listed in the SORN that does not need to be included in the summary would be that the system does not regularly handle requests from Congressional members.

5.1.4 For each interface with a system outside the Department, state what specific information is shared with each specific partner. For example, Customs and Border Protection may share biographic information on an individual with the Federal Bureau of Investigation.

5.1.5 Where you have a specific authority to share the information, please provide a citation to the authority and statute name.

5.2 Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of DHS.

5.2.1 What legal mechanisms, authoritative agreements, documentation, or policies are in place detaling the extent of the sharing and the duties of each party? If an Memorandum of Understanding (MOU) or other formal agreement is not in place, is the sharing covered by a routine use in the SORN and does it comply with the routine uses? If not, explain the steps being taken to address this omission.

5.3 How is the information shared outside the Department and what security measures safeguard its transmission?

5.3.1 Is the information shared in bulk, on a case by case basis, or does the organization have direct access to the information?

5.3.2 Describe how the information is transmitted to entities external to the Department and whether it is transmitted electronically, by paper, or some other means.

5.3.3 If specific measures have been taken to meet the requirements of OMB Memorandums M-06-15 and M-06-16 please note them here.

5.3.4 Any sharing conducted per a routine use in the applicable SORN should be transmitted in a secure manner. Additionally, if information is shared pursuant to an MOU, Memorandum of Agreement (MOA), or similar formal agreement, please discuss if and how the agreement requires secured transmission and storage of shared data.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

5.4.1 Please discuss how the uses of the information are in accord with the stated purpose and use of the original collection. If use has expanded since the initial collection, explain how appropriate notice has been given to the affected individuals.

5.4.2 For example, if an MOU, contract, or agreement is in place, what safeguards (including training, access controls, and security measures) are in place at the external agency to ensure information is used appropriately?

Section 6.0
Notice

The following questions are directed how or whether the individual is notified of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Was notice provided to the individual prior to the collection of information?

6.1.1 This question is directed at the notice provided prior to collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the *Federal Register*. If notice was provided in the *Federal Register* please provide the citation. If notice was not provided, explain why.

6.1.2 If yes, please provide a copy of the current notice.

6.1.3 Describe how the notice provided for the collection of information is adequate to inform those impacted by the system that their information has been collected and is being used appropriately. Discuss any notice provided on forms or on web sites associated with the collection.

6.1.4 The issue of notice, particularly notice found in a System of Records Notice, involves the advice of counsel. Please consult your assigned counsel on issues concerning the sufficiency of notice to the public regarding an information collection.

6.2 Do individuals have the opportunity and/or right to decline to provide information?

6.2.1 This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

6.3.1 This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his/her information. If specific consent is required, how would the individual consent to each use?

6.4 Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

6.4.1 Discuss how the notice provided corresponds to the purpose of the program or system and the stated uses. How is the notice appropriate given how the system is designed?

6.4.2 Also, please discuss how the uses of the information and the notice given for the initial collection are in accord with the stated use of the information.

Section 7.0
Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the

information collected about them.

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

7.1.1 Cite any procedures or regulations your component has in place that allow access to information. These procedures, at a minimum, should include the Department's FOIA/Privacy Act practices but may also include additional access provisions. 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.

7.1.2 If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

7.1.3 If the system is not a Privacy Act system, please explain what procedures and/or regulations are in place that cover an individual gaining access to his/her own information.

7.2 What are the procedures for correcting inaccurate or erroneous information?

7.2.1 Discuss the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, please state as much.

7.3 How are individuals notified of the procedures for correcting their information?

7.3.1 How is an individual made aware of the procedures for correcting their information? This may be through notice at collection, or through other similar means. 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 signficantly.

7.4 If no formal redress is provided, what alternatives are available to the individual?

7.4.1 Redress is the process by which an individual gains access to his/her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and/or Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

7.5.1 Discuss how the redress and access measures offered in the system and collection of information are appropriate given the purpose of the system. For example, if the minimal redress procedures provided in the Privacy Act and the Freedom of Information Act were deemed inadequate please explain why the additional redress measures offered are beneficial to the system.

7.5.2 For example, some systems allow user access to information and the ability of the individual to correct or alter his/her information. This ensures data accuracy and improves the system to functions by increasing confidence in the integrity of the data. However, if a system does not allow individual access, this needs to be analyzed as an accepted risk in light of the purpose of the system.

Section 8.0
Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system and are they documented?

8.1.1 Descibe the process by which an individual receives access to the system.

8.1.2 Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system.

8.1.3 Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

8.2 Will Department contractors have access to the system?

8.2.1 How frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

8.3.1 DHS and its components offer privacy and security training. Each program or system may offer training specific to the program or system which touches on information handling procedures and sensitivity of information. Please discuss how individuals who have access to personally identifiable information are trained to appropriately handle it.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

8.4.1 Please provide the date that the Authority to Operate (ATO) was granted. An operational system should be in compliance with Management Directive 4300A. Please note that all systems containing personally identifiable information are categorized at a minimum "moderate" under Federal Information Processing Standards Publication 199.

8.5 What auditing measures and technical safeguards are in place to prevent misuse of data?

8.5.1 This question is designed to allow the drafter to discuss the security measures that support the program or system. Robust auditing measures are common and should

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

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

8.6 Privacy Impact Analysis: Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

8.6.1 Please discuss the particular security risks presented by the system and how they have been mitigated. Do not discuss in such detail as to compromise security measures, but please discuss how the security measures enabled for the system (user access controls, auditing, etc.) help mitigate any potential risk to the security of the system or the privacy of the information it contains.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

9.1.1 The Department undertakes a variety of different types of projects utilizing a variety of technologies. Some possible project types include: operational, pilot, basic research, toolset, and infrastructure.

9.2 What stage of development is the system in and what project development life cycle was used?

9.2.1 Please indicate in which stage your project is. Whether the project is basic research or the project supports operational systems, some form of development life cycle should be used. Please describe the stage at which the project is currently operating.

9.2.2 Was the system assessed through the Department's technology investment review process including the Enterprise Architecture Center of Excellence (EACOE) and Integrated Project Review Team (IPRT)? If so, what was the result? Were business requirements gathered? If so, please summarize. Was a data dictionary and/or data reference model developed? Was a process flow diagram developed for this system?

9.3 Does the project employ technology which may raise privacy concerns? If so please discuss its implementation.

9.3.1 In addition to the devevlopment life cycle and the particular stage of development a system is in, the technology chosen to accomplish program and system goals drive specific issues concerning privacy. Individual types of technology may raise discrete privacy issues and it is important to identify these issues early in any development cycle. Please discuss the issues inherent to the particular technology chosen.

Approval and Signature Page

Provide a contact name and number for the component Privacy Officer, program manager, or system owner of the operation, technology, or rule 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.

Questions? Contact Us.

Privacy Office

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

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

Appendix I
PIA Triggers

After completing a PTA, please consult with the Privacy Office to determine whether a PIA is required and to identify any existing PIAs or SORNs for the system. According to OMB Memorandum M-03-22, the system activities listed below may require a PIA:

Alteration in Character of Data

when personally identifiable information is added to a collection and risks to personal privacy are raised. For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise.

Anonymous to Non-Anonymous

when functions applied to an existing information collection change anonymous information into personally identifiable information;

Commercial Sources

when agencies systematically incorporate into existing information systems databases of personally identifiable information purchased or obtained from commercial or public sources (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);

Conversions

when converting paper-based records to electronic systems;

Internal Flow or Collection

when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system additional items of personally identifiable information;

New Interagency Uses

when agencies work together on shared functions involving significant new uses or

exchanges of personally identifiable information, such as the cross-cutting E-Government initiatives (in such cases, the lead agency should prepare the PIA);

New Public Access

when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;

Significant Merging

when agencies adopt or alter business processes so that government databases holding personally identifiable information are merged, centralized, matched with other databases or otherwise significantly manipulated:

For example, when databases are merged to create one central source of information, such a link may aggregate data in ways that create new privacy concerns.

Significant System Management Changes

when new uses of an existing IT system, including application of new technologies, significantly change how personally identifiable information is managed in the system:

For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores, such additions could create a more open environment and avenues for exposure of data that previously did not exist.

Privacy Office Staff

Hugo Teufel III
Chief Privacy Officer &
Chief FOIA Officer

Kenneth P. Mortensen
Deputy Chief Privacy Officer

Catherine Papoi
Deputy Chief FOIA Officer and Director,
Departmental Disclosure & FOIA

Toby Milgrom Levin
Senior Advisor

John Kropf
Director, International Privacy Policy

Peter Sand
Director, Privacy Technology

Rebecca J. Richards
Director, Privacy Compliance

Ken Hunt
Director, Legislative and Regulatory
Analysis

Sandra L. Hawkins
Administrative Officer

Shannon Ballard
International Privacy Analyst

Lauren Saadat
International Privacy Analyst

Lane Raffray
Special Assistant to the Chief Privacy Officer

Nathan Coleman
Privacy Assessment Coordinator

Vania Lockett
Deputy Director, Departmental
Disclosure & FOIA

William Holzerland
Deputy Director, Departmental
Disclosure & FOIA

Mark Dorgan
FOIA Specialist

Privacy Office Contract Support

Cathy Lockwood
Senior Policy Analyst

Bob Moll
Senior Policy Analyst

Brooke Dickson-Knowles
Privacy Analyst

Rachel Drucker
Privacy Analyst

Shannon Kelso
Privacy Analyst

Tamara Baker
Privacy Analyst

Sandra Debnam
Administrative Assistant

Kathleen Pianka
Administrative Assistant

Stephanie Kuehn
FOIA Specialist

Loren Clark-Moe
FOIA Specialist
Emily McMullen
FOIA Specialist
Ryan Witt
FOIA Specialist
Carol Curley
FOIA Specialist
Erin Odom
FOIA Processor

Component Privacy Officers

Peter Pietra
Privacy Officer, TSA
Claire Miller
Acting Privacy Officer, US-VISIT
Elliot Avivian
Acting Privacy Officer, S&T