Privacy Impact Assessments

Official Guidance

The Privacy Office

Homeland Security

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
March 2006

Dear Colleagues,

In the following pages you will find the Department's Guidance on drafting Privacy Impact Assessments (PIA), as required under the E-Government Act of 2002 and the Homeland Security Act of 2002.

The Privacy Office is available to answer questions that you may have as you develop your programs, technical systems, and PIAs. Chances are that if you are starting a Privacy Impact Assessment you have already spoken with us, but if that is not the case please contact our Director of Privacy Compliance, Rebecca J. Richards, with any questions you may have in completing a PIA.

The Privacy Impact Assessment can be one of the most important instruments in establishing trust between the Department's operations and the public. Conducting PIAs in connection with program and information system development demonstrates the Department's forward efforts to assess the privacy impact of utilizing new or changing information systems, including attention to mitigating privacy risks. This PIA guidance is provided to better assist you in that effort.

Establishing a culture of privacy attentiveness reflects state-of-the-art information management practices, as well as good government practices. Thank you for the important role you play in integrating privacy attentiveness into the way in which we carry out the Department's mission.

Respectfully,

Maureen Cooney
Acting 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 Privacy Impact Assessments (PIA) for all new or substantially changed technology that collects, maintains, or disseminates personally identifiable information.

The Chief Privacy Officer of the Department of Homeland Security is required by Section 222 of the Homeland Security Act to ensure that the technology used by the Department sustains privacy protections. The Privacy Impact Assessment 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 offices and programs.

In 2004, the Department of Homeland Security Privacy Office issued *Privacy Impact Assessments Made Simple*. This amended guidance, *Privacy Impact Assessment Guidance* 2006, supersedes *PIAs Made Simple* and any previously issued Guidance. This Guidance reflects the 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.

What is a PIA?

A PIA is an analysis of how personally identifiable information is collected, stored, protected, shared and managed. "Personally identifiable information" is defined as information in a system or online collection that directly or indirectly identifies an individual whether the individual is a U.S. Citizen, Legal Permanent Resident, or a visitor to the U.S. In some cases, personal information, such as a body scan, may be captured only for a short period of time. This is still considered a collection, however, and a PIA would need to be conducted during the development and prior to the deployment of the new technology.

The purpose of a PIA is to demonstrate that system owners and developers have consciously incorporated privacy protections throughout the entire life cycle of a system. This involves making certain that privacy protections are built into the system from the start, 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 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 and intelligence 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 personal information that we collect, store, retrieve and share.

These protections, embodied in Federal law, 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. The E-Government Act of 2002 mandates an assessment of the privacy impact of any substantially revised or new information technology system because of the potential privacy impacts from maintenance of electronic databases. Similarly, the Homeland Security Act of 2002 acknowledges the Department's role in collecting sensitive information about individuals and includes a requirement that the Chief Privacy Officer of the Department ensure that technology used by the Department sustains privacy protections. The Homeland Security Act also recognizes the potential effect of proposed rules on privacy and authorizes the Chief Privacy Officer to conduct privacy impact assessments on proposed rules of the Department.

The document in 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 personal 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 the technology and/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 a system's development and throughout the system's life cycle. The PIA process and the document itself are intended to ensure that privacy protections are built into the system

from the start, not after the fact when privacy concerns can be far more costly to address or could affect the viability of the project. Additionally, the PIA demonstrates that the system developers and owners have made technology choices that reflect the incorporation of privacy into the fundamental system architecture. In order to make the PIA comprehensive and meaningful, it should involve collaboration between program, information technology, security, and privacy experts.

The PIA is a living document that needs to be updated regularly as the program and system are developed, not just when the 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.

Under the E-Government Act, 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.

Under the Homeland Security Act of 2002, the Chief Privacy Officer is charged with ensuring that the Department uses technologies that sustain and do not erode privacy. Part of this charge is fulfilled by requiring that agencies complete PIAs for all new technologies, new collections of personal information, and new systems or existing systems that are being substantially updated. The statute also requires that agencies conduct PIAs on all new rulemakings that could impact privacy. By following this guidance, the PIA requirement will be fulfilled.

Information Covered by the PIA

A PIA should be completed for any system, program, technology or rulemaking that involves personally identifiable information. Personally identifiable information is information in a system, online collection, or technology: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. As found in OMB

Memorandum M-03-22, these data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. In some cases a system or technology may only momentarily collect information about an individual, such as a surveillance camera. A PIA is required for the acquisition of such a new technology. In other cases, the technology may not be changing, but a program decides to use data from a new source such as commercial aggregator of information. A PIA is required when such new sources of information are used.

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, 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.

In some cases the technology may only collect personal 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 would be required. Examples of technology with privacy implications could include systems utilizing radio frequency identification devices (RFID), biometric scans, data mining, or geospatial tracking.

Example of new data collections with privacy implications:

Your agency is beginning to collect personal information in order to conduct a program to review individuals who volunteer for a pre-approved traveler program. This is a new collection of information, despite the information being voluntarily given by individuals. Such a collection would require a PIA.

Regarding "Private" Information

Personally identifying 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 identifying 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 "personal information."

Example: A license plate number is personally identifying 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) that describe the categories of personally identifiable information that they collect, maintain, retrieve, and use. Generally, the requirements to conduct a PIA are broader and more frequent than the requirements for System of Records Notices. The PIA requirement is triggered by both the technology and the collection of information. 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 changing, a PIA must be completed or updated to reflect the new impact of the technology.

The PIA requirement does not provide an exemption for pilot testing programs. If the system is being designed to handle personal information even in a pilot test, the PIA is required to be published prior to the commencement of any pilot test. If in the process of developing a new program, a SORN needs to be updated, a PIA will also be required.

When to Conduct a PIA

A PIA should be conducted when an office is doing any of the following:

- Developing or procuring any new technologies or systems that handle or collect personal 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 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 adds additional sharing of information either with another agency or incorporating commercial data from an outside data aggregator, a PIA a required. Appendix I of this document provides extensive examples.
- Issuing a new or updated rulemaking that affects personal 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 program has specific authority to collect certain information or build a certain program, a PIA is required.

Classified Information and Systems

A PIA should be conducted for all systems handling personally identifiable information, including classified systems, but the program may be exempted from the requirement to publish the PIA. Note that Privacy Office personnel are cleared to read classified materials, and prior to public release of any PIA, all proper redactions will be made.

Privacy Threshold Analysis

Some information systems will not require a full PIA. For efficiency a system owner or program manager can be aided in making the determination of whether a full PIA is required by conducting and following a Privacy Threshold Analysis (PTA). For any system within the Department a PTA should be conducted in order to determine if a full PIA is necessary.

A PTA contains six basic questions about the nature of the system in addition to a basic system description. The questions are as follows:

I. Was the system developed *prior* to 2002? (Yes/No)

(If the answer is "yes" proceed to Question 2.)
(If the answer is "no", proceed to Section II.)

1. Has the system undergone any significant changes since 2002? (If "yes," please continue to Question 2.)

(If "no," the PTA is complete and should be sent to the Privacy Office)

2. What changes were made to the system since 2002? (Answer and continue to Question 3)

3. Does the system collect, maintain and/or share information that can be used to directly or indirectly identify an individual?

(If the answer to Question 3 is "yes" a full PIA is required.)
(If the answer is "no" the Threshold Analysis is complete. Please send to the Privacy Office.)

II. Was the system developed *after* 2002? (Yes/No)

1. What is the purpose of the system? (Answer in detail and proceed to Question 2.)

2. What information does the system collect, maintain, or share?

3. Does the system collect, maintain and/or share information that can be used to directly or indirectly an individual?

(If the system was developed after 2002, and the answer to Question 3 is "yes" a full PIA is required.)
(If the answer is "no" the Threshold Analysis is complete. Please send to the Privacy Office.)

PTAs are currently incorporated into the Certification & Accreditation (C & A) process, which is the process by which the Department assures its systems meet appropriate system and operating standards. Through the C & A process the Privacy Office reviews PTAs submitted by each program and/or system. The official version of the PTA can also be obtained from the Privacy Office or component Privacy Officers.

A properly completed and approved PTA provides documentation that a system owner thought through privacy concerns whether or not a full PIA is deemed to be required. A PTA provides a foundation for a full PIA should one be required.

How to Conduct a PIA

Section 208 of the E-Government Act of 2002 states that agencies are required to conduct PIAs for electronic information systems and collections. The Act 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 system. Any new system development that involves the processing of personal information should be able to demonstrate, through the PIA, that an in-depth analysis was done to ensure that privacy protections were built into the system.

In order to give Department PIAs consistency, documents should use the Department of Homeland Security PIA Template which is available through the Privacy Office. 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 state that it is not applicable and the justification.

Please adhere to the following guidelines when drafting a PIA:

- Draft PIAs from the perspective of a member of the public who knows nothing about the system, technology, or rulemaking.
- Spell out each acronym the first time you use it in the document. For example: Office of Management and Budget (OMB).
- Use words, phrases, or names in the PIA that are readily known to the average person.
- Technical terms or references should be defined.
- Clearly reference projects and systems and provide explanations, if needed, to aid the general public.
- References to National Institute of Science and Technology (NIST) publications and other documents should include the complete name of the reference (e.g., 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.

Writing Guidance

Guide to Template for Privacy Impact Assessment

Writing the PIA

A Privacy Impact Assessment Template has been developed for ease of use, which includes only the top level questions noted below. The sublevel questions and examples in the below outline are to provide you with additional guidance in responding to the required questions. The Template is available on the Privacy Office website at www.dhs.gov/privacy and by following the link to the Privacy Impact Assessment section.

Introduction

The introduction should contain the following elements, and should not exceed one page:

- The system name, the unique system number if there is one, and the name of the Department component(s) that own(s) the system;

- The objective of the new program, technology and/or system and how it relates to the component's and Department's mission;
- A general description of the information in the system and the functions the system performs that are important to the component's and the Department's mission; and
- A general description of the modules and subsystems, where relevant, and their functions. For longer more in depth descriptions, an appendix may also be appropriate.

A clear and concise introduction provides an overview of the system and gives the reader the appropriate context in which to view the remainder of the PIA.

Section 1.0
The System and the Information Collected and Stored within the System.

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 system, rule, and/or technology being developed.

1.1 What information is to be collected?

1.1.1 Identify and list all personal 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 address, facsimile number, 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 number, 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 In some cases, a general summary of the information may be put in the first section and an appendix with the full list may be added to the back of the PIA.

1.2 From whom is the information collected?

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 is using data from a commercial aggregator of information, state the fact that this is where the information is coming from and then in 1.3 indicate why the program is using this source of data.

1.3 Why is the information being collected?

1.3.1 In responding to this question, you should include:

1.3.1.1 A statement of why this PARTICULAR personally identifiable information that is collected and stored in the system is necessary to the component's or to the 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.

1.3.1.2 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.

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

Privacy Impact Analysis: Given the amount and type of data collected, discuss what privacy risks were identified and how they were mitigated. For example, if during the design process, a decision was made to collect less data, include a discussion of this decision.

Section 2.0
Uses of the System and 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.

2.1.2 If a SORN has been published for the system, the routine uses from the SORN should be described in this section. In addition, list the uses internal to the Department since the routine uses listed in the SORN are limited to disclosures made outside of the Department.

2.1.3 Do not list the routine uses directly from the SORN, summarize the most relevant ones. For example, if the system does not regularly handle requests from Congressional members, this does not need to be included in the summary. If instead, the system provides full access to another agency for their use of the information, this should be discussed in this section.

2.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

2.2.1 Many systems sift through large amounts of information in response to a user inquiry or programmed functions. This is loosely known as data mining. When these systems sift through information they make determinations and, sometimes, conclusions based upon the information they analyze. If the system being analyzed in the PIA conducts such preliminary and conclusory functions, please provide greater detail on what type of determinations the system makes.

2.2.2 If the system creates or makes available new or previously unavailable information about an individual, state/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 what circumstances that information will be used and by whom.

2.3 How will the information collected from individuals or derived by the system, including the system itself be checked for accuracy? In responding to this question address the following where applicable:

2.3.1 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.

2.3.2 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.

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. For example, is appropriate use of information covered in training for all users of system? Are strict disciplinary programs in place if an individual is found to be inappropriately using the information?

Section 3.0
Retention

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

3.1 What is the retention period for the data in the system?

3.2 Has the retention schedule been approved by the National Archives and Records Administration (NARA)?

Privacy Impact Analysis: Considering the purpose for retaining the information, explain why the information is maintained for the indicated period.

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?

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.

4.2 For each organization, what information is shared and for what purpose?

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

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

4.2.3 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.

4.3 How is the information transmitted or disclosed?

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

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

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?

5.1.1 The term "external" references other departments, agencies and organizations that are not a part of the Department. 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.

5.2 What information is shared and for what purpose?

5.2.1 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 its information on an individual with the Federal Bureau of Investigation (FBI).

5.2.2 Where you have a specific authority to share the information, please provide a citation to the authority.

5.3 How is the information transmitted or disclosed?

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 Describe if the information sent to or from external entities is transmitted electronically, by paper, or some other means.

5.4 Is a Memorandum of Understanding (MOU), contract, or agreement in place with any external organization(s) with whom information is shared, and does the MOU reflect the scope of the information currently shared?

5.4.1 If an MOU is not in place, is the sharing covered by a routine use in the System of Records Notice? If not, explain the steps being taken to address this omission.

5.5 How is the shared information secured by the recipient?

5.5.1 For each interface with a system outside the Department:

5.5.1.1 Identify and list who is responsible for assuring the security and privacy of the data once it is shared; and if possible, include a reference to and quotation from any MOU, contract, or other agreement that defines the parameters of the sharing agreement.

5.5.1.2 Explain whether the external system has a certification & accreditation (C & A) under Federal Information Security Management Act (FISMA) or other relevant computer security standards. If the external system has not completed C & A, how have the external system's security issues been addressed to ensure the privacy and security of the information once it is shared?

5.6 What type of training is required for users from agencies outside the Department prior to receiving access to the information?

Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated. For example, if an MOU, contract, or agreement is in place, what safeguards (including training, access controls, and security measures) have been implemented by the external agency to ensure information is used appropriately.

Section 6.0
Notice

The following questions are directed at notice to the individual 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 If yes, please provide a copy of the notice. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a System of Records Notice published in a Federal Register Notice. If notice was not provided, explain why not.

6.1.2 Question 6.1 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 being collected.

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

6.2.1 Question 6.2 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 Question 6.3 is directed at whether the consent given to the collection of information covers all uses (current or potential) of their information or if an individual may provide consent for specific uses. If such consent is required, how would the individual consent to each use.

Privacy Impact Analysis: Conspicuous and transparent notice allows individuals to understand how their information will be used and disclosed. Describe how notice for the system was crafted with these principles in mind. For example, if a traditional System of Records Notice was not deemed sufficient to inform the public, include a discussion of the decision to provide expanded notice.

Section 7.0
Individual 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 would be in addition to the Department's FOIA/Privacy Act practices. 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 amendment/correction provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found.

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.

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

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).

Privacy Impact Analysis: Discuss whether and how individual redress is provided in light of the Privacy Act of 1974 and the Freedom of Information Act. For example, if redress procedures provided in the aforementioned statutes we deemed inadequate, describe what types of redress procedures were implemented and why.

Section 8.0
Technical Access and Security

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

8.1 Which user group(s) will have access to the system?

8.1.1 Identify and list the types of users. For example: managers, system administrators, contractors, and developers may have access to the system.

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

8.2 Will contractors to the Department have access to the system?

8.2.1 If so, please submit a copy of the contract describing their role to the Privacy Office with this PIA.

8.3 Does the system use "roles" to assign privileges to users of the system?

8.3.1 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 able to make certain amendments or changes to the information.

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

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

8.5.1 For example, when an employee no longer works for the organization or in a specific job function, there is a set procedure for removing access in timely.

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

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

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Privacy Impact Analysis: Given the sensitivity and scope of information collected, what privacy risks were identified and mitigated. For example, were decisions made to encrypt certain data sets and not others.

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 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

9.3 What design choices were made to enhance privacy?

Conclusion

The concluding section should inform the reader, in a summary fashion, how you constructed your system, program, rule, or technology based on privacy risks and mitigation strategies.

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.

Questions? Contact Us.

Privacy Office

U.S. Department of Homeland Security
Arlington, VA 22202

Email: PIA@dhs.gov
Phone: 571-227-3813
Web Site Link: www.dhs.gov/privacy

Appendix I
PIA Triggers

After completing a Privacy Threshold Analysis, please consult with the Privacy Office to determine whether a Privacy Impact Assessment (PIA) is required and to identify any existing PIAs or System of Records Notices (SORNs). According to OMB Memorandum M-03-22, the system activities listed below may require a PIA:

Conversions

when converting paper-based records to electronic systems;

Anonymous to Non-Anonymous

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

Significant System Management Changes

when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form 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.

Significant Merging

when agencies adopt or alter business processes so that government databases holding information in identifiable form 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 privacy concerns not previously at issue.

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;

Commercial Sources

when agencies systematically incorporate into existing information systems databases of information in identifiable form 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);

New Interagency Uses

when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;

Internal Flow or Collection

when alteration of a business process results in significant new uses or

disclosures of information or incorporation into the system of additional items of information in identifiable form;

Alteration in Character of Data

when new information in identifiable form added to a collection raises the risks to personal privacy. For example, the addition of health or financial information may lead to additional privacy concerns that otherwise would not arise.

Privacy Office Staff

Maureen Cooney
Acting Chief Privacy Officer &
Chief FOIA Officer

Sandra L. Hawkins
Administrative Officer

Elizabeth Withnell
Chief Counsel to the Privacy Office

Toby Milgrom Levin
Senior Advisor

Kenneth P. Mortensen
Senior Advisor

Tony Kendrick
Director, Departmental Disclosure & FOIA

John Kropf
Director, International Privacy Programs

Peter Sand
Director, Privacy Technology

Rebecca Richards
Director, Privacy Compliance

Billy Spears
Director, Privacy Education & Training

Catherine Papoi
Deputy Director, Departmental
Disclosure & FOIA

Erica Perel
Attorney-Advisor

Lane Raffray
Privacy Policy Analyst

Anna Slomovic
Senior Privacy Strategist

John Sanet
Senior Privacy Advisor

Nathan Coleman
Privacy Analyst

Kathleen Kavanaugh
Privacy Researcher

Tamara Baker
Event Executive

Sandra Debnam
Administrative Assistant

Erin Odom
Administrative Assistant

Vania Lockett
Senior FOIA Specialist

Rasheena Spears
FOIA Specialist

Stepahnie Kuehn
FOIA Specialist

Mark Dorgran
FOIA Specialist

Shannon Snypp
FOIA Specialist

Component Privacy Officers

Lisa Dean
Privacy Officer, TSA

Elizabeth Gaffin
Privacy Officer, CIS

Andy Purdy
Privacy Officer, NCSD

Steve Yonkers
Privacy Officer, US-VISIT

The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528
571-227-3813
www.dhs.gov/privacy
Email address: PIA@dhs.gov