PRIVACY IMPACT ASSESSMENTS

Official Guidance

Privacy and Civil Liberties Office

Office of the Deputy Attorney General

Revised August 7, 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.

The Privacy and Civil Liberties 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 Privacy Compliance Counsel, Niels Quist, with any questions you may have when 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,

Jane C. Horvath
Chief Privacy and Civil Liberties Officer
Department of Justice

Introduction

Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new technology involving the collection, maintenance or dissemination of information in identifiable form or that make substantial changes to existing technology for managing information in identifiable form. The Office of Management and Budget ensures that PIAs for major information systems (MIS) necessitated under the E-Government Act are completed by requiring them as part of the annual budget process. Agencies are required to provide OMB with a copy of the PIA for an information technology system for which a PIA is required and for which funding is requested.

This policy is solely for the purpose of setting forth internal Department policy, and does not create any rights, substantive or procedural, that are enforceable at law by any party in any matter, civil or criminal.

What is a PIA?

A PIA is an analysis of how information in identifiable form is collected, stored, protected, shared, and managed in an IT system or online collection.

The purpose of the PIA is to analyze how an agency handles information in order to: 1) ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) determine the risks and effects of collecting, maintaining, and disseminating information; and 3) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks. The PIA ensures 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, the component privacy officer, and the Privacy and Civil Liberties Office ("PCLO") 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 Justice.

Complying with the PIA Requirement

The Department of Justice is committed to analyzing and sharing information and intelligence through all of its agencies. At the same time, the Department should have in place robust protections for the privacy of any information in identifiable form 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 while still executing the Department's mission;

- Maximize fairness in institutional decisions made about individuals; and

- Observe reasonable expectations of individual privacy and safeguard personally identifiable information.

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.

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. 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 document that may need to be updated 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 Department of Justice Reauthorization Act of 2005, the Chief Privacy and Civil Liberties 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.

Information Covered by the PIA

A PIA should be completed for any IT system or online collection that involves the collection, maintenance, or dissemination of information in identifiable form. "Information in identifiable form" is defined as information in an IT system or online collection: (i) that directly identifies an individual[1] (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or

[1] For purposes of conducting PIAs, it is the Department's policy to define "individual" in this context as any natural person regardless of citizenship status.

(ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification (e.g., a combination of gender, race, birth date, geographic indicators, and/or other descriptors).

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 groups of records that agencies maintain from which information about U.S. citizens and lawfully admitted permanent resident aliens is retrieved by such individuals' personal identifiers. 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 in a manner that creates new privacy risks, 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 information in identifiable form, 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 may 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 IT systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public.[2]
- Initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities, or employees of the federal government).
- Changing an existing system in a manner that creates new privacy risks. For example:
  - when converting paper-based records to electronic systems;
  - when changing anonymous information into information in identifiable form;
  - when new uses of an IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system;
  - when merging, centralizing, or matching databases that contain information in identifiable form with other databases, or when otherwise significantly manipulating such databases;
  - when newly applying any user-authenticating technology to an electronic information system that is accessed by members of the public;
  - when systematically incorporating into existing information systems

[2] 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.

databases of information in identifiable form that are purchased or obtained from commercial or public sources;
- when working with another agency or agencies on shared functions that involving significant new interagency uses or exchanges of information in identifiable form;
- when altering a business process that results in significant new uses or disclosures of information or the incorporation into the system or addition items of information in identifiable form; or
- when adding new information in identifiable form, the character of which raises the risks to personal privacy (for example, adding health or financial information)

When a PIA is NOT Required

No PIA is required where information:
- has been previously assessed under an evaluation similar to a PIA; or
- where privacy issues are unchanged.

Examples of when a PIA would not be required:
- For government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback or obtaining additional information;
- When all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act of 1974;
- When all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and the resulting data is protected under Title V of the E-Government Act of 2002;
- When developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generate information in identifiable form;
- For minor changes to a system or collection that do not create new privacy risks.

UPDATING PIAs

Agencies must update their PIAs to reflect changed information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form.

Classified Information and Systems

It is the Department's policy that a PIA should be conducted for all systems handling information in identifiable form, including classified systems, but the program may be exempted from the requirement to publish the PIA. Note that PCLO personnel are cleared to read classified materials, and prior to public release of any PIA, all proper redactions will be made.

Privacy Threshold Analysis

For efficiency, a system owner or program manager can be aided in making the

determination of whether a PIA is required by conducting and following a Privacy Threshold Analysis (PTA).

A PTA contains 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 April 17, 2003? (Yes/No)

(If the answer is "yes" proceed to Question 1.)

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

1. Has the system undergone any significant changes since April 17, 2003? (If "yes," please explain the nature of those changes and please continue to Question 2.)
   (If "no," the PTA is complete and should be sent to the PCLO.)

2. Do the changes involve the collection, maintenance, or dissemination of information in identifiable form about individuals?
   i. (If the answer to Question 2 is "yes" proceed to Question 3.)
   ii. (If the answer is "no" the Threshold Analysis is complete. Please send the PTA to the PCLO.)

3. Is the system solely related to internal government operations?
   i. (If the answer to Question 3 is "yes", please provide a brief explanation of the purpose of the system, the quantity and type of employee/contractor information collected, and whether the system is a Major Information System. If the system is a Major Information System, a full PIA is required. If the system is not a Major Information System, PCLO reserves the right to require a component to conduct a PIA for a system that only collects information on employees/contractors. In either case, please forward the completed PTA to the PCLO.)
   ii. (If the answer to Question 3 is "no" go to subsection III to determine if a full or short-form PIA is required.)

II. For systems developed after April 17, 2003.

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

2. Does the system collect, maintain or disseminate information in identifiable form about individuals?
   i (If the answer to Question 2 is "yes" please proceed to Question 3.)
   ii (If the answer is "no" the Threshold Analysis is complete. Please send the PTA to the PCLO.)

3. Is the system solely related to internal government operations?
   i. (If the answer to Question 3 is "yes", please provide a brief explanation of the purpose of the system, the quantity and type of employee/contractor information collected, and whether the system is a Major Information System. If the system is a Major Information System, a full PIA is required. If the system is not a Major Information System, PCLO reserves the right to require a component to conduct a PIA for a system that only collects information on

employees/contractors. In either case, please forward the completed PTA to the PCLO.)

ii. (If the answer to Question 3 is "no" go to subsection III to determine if a full or short-form PIA is required.)

III. Full or Short-Form PIA

1. Is the system a major information system?
   i. (If "yes", a full PIA is required.)
   ii. (If "no", please continue to question 2.)
2. Does the system involve routine information AND have limited use/access? Please explain what type of information is collected and the access provided. Please note that the reviewing official has the right to require the component complete a full PIA.
   i. (If "yes", a short-form PIA is required. You need only answer Questions 1.1, 1.2, 2.1, 3.1, 4.1, 5.1 (if appropriate), 6.2, 6.3, and 8.9.)
   ii. (If "no", a full PIA is required.)

The most current version of the PTA can be obtained from the PCLO or the Senior Component Official for Privacy.

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. Provided, however, that agencies, in their discretion are not required to make a PIA publicly available if it would raise security concerns or reveal classified (i.e., national security) information, or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) that is contained in the assessment. Nonetheless, 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 information in identifiable form 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.

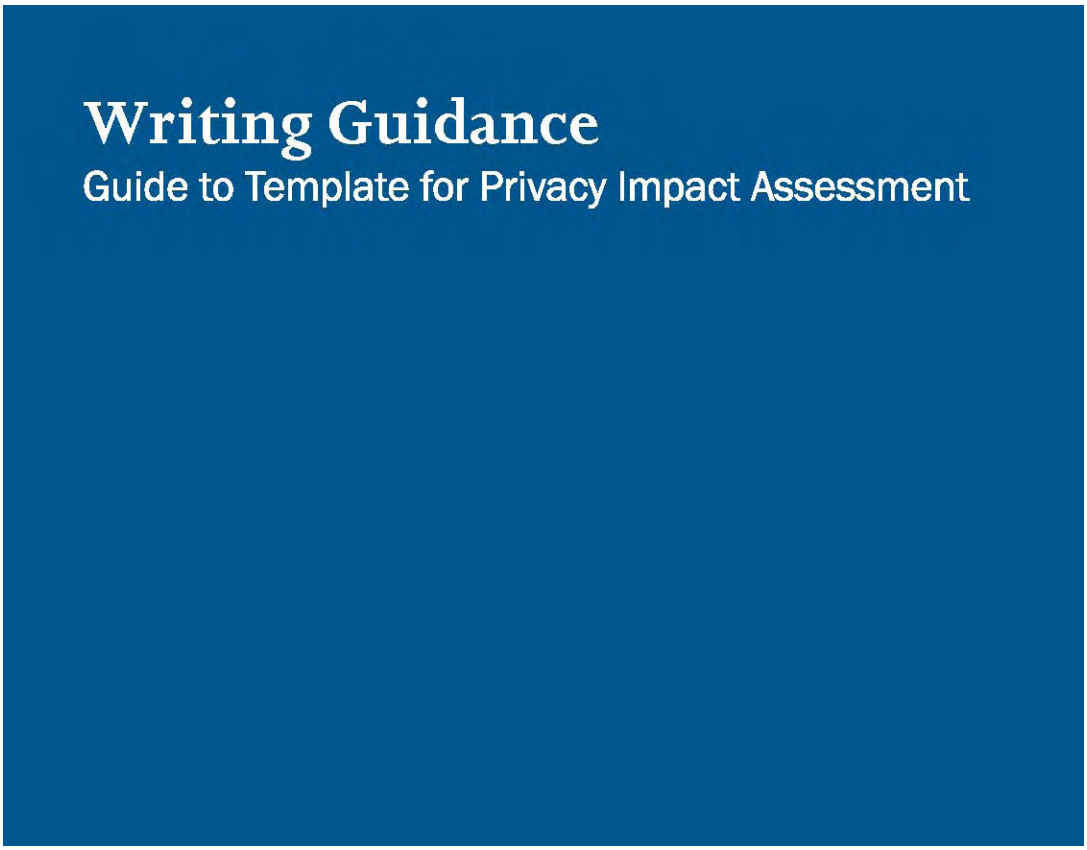
In order to give Department PIAs consistency, documents should use the Department of Justice PIA Template which is available through the PCLO website, your component's Senior Component Official for Privacy, or on the DOJnet. All PIAs completed after the effective date of this amended guidance should 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 taking into account 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 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 PCLO website located on the DOJ Website 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 in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

1.1.1 Identify and list all of the types of information in identifiable form that are collected and stored in the system that either directly identify an individual (such as name, address, social security number, telephone number, e-mail address, biometric identifiers, photograph, or other unique identifying number, code, or characteristic) or that when combined, indirectly identify an individual (such as a combination of gender, race, birth date, geographic indicator, license number, vehicle identifier including license plate, and other descriptors).

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 in the case of an investigator taking a statement from a suspect, 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 systematically incorporating databases of information in identifiable form that are purchased or obtained from a commercial aggregator of information or if information needs to be collected from third parties in an ongoing investigation, state the fact that this is where the information is coming from and then in 2.1 indicate why the program is using this source of data.

Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.

2.1 Why is the information being collected?

2.1.1 In responding to this question, you should include:

2.1.1.1 A statement of why this PARTICULAR information in identifiable form 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 information in identifiable form should be collected and stored is not an adequate response to this question.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

2.3 *Privacy Impact Analysis*: Given the amount and type of data collected, as well as the purpose 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 3.0 Uses of the System and the Information

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

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

3.1.2 If a SORN is being or has been published for the system, the routine uses from the SORN should be listed in this section. (A copy of the notice or its Federal Register citation may be provided in order to meet this requirement.) 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.

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

3.2.1 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.

3.2.2 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.

3.3 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:

3.3.1 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 determinations 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.

3.3.2 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.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

3.5. *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 and describe why the information is being retained for the indicated period. 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 4.0 Internal Sharing and Disclosure of Information within the System

The following questions are intended to describe the scope of sharing both within the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

4.1.1 Identify and list the name(s) of any components, offices, and any other

organizations within the Department with which the information is shared.

4.2 For each recipient component or office, what information is shared and for what purpose?

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

4.2.2 Identify the specific information that is shared with the specific component office, or organization within the Department and the purpose served by such sharing.

4.3 How is the information transmitted or disclosed?

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

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

4.4 *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 component, office, or organization has access to the system that your office 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 (non-DOJ) recipient(s) is the information shared?

5.1.1 Identify and list the name or names of the foreign, federal, state, or local government agencies, private sector organizations, or individuals with which/whom the information is shared.

5.2 What information is shared and for what purpose?

5.2.1 Identify the specific information that is shared with each specific recipient and the purpose served by such sharing. For example, the Federal Bureau of Investigation (FBI) may share its information on an individual with Customs and Border Protection. If you provided a list of routine uses in response to Question 3.1, please reference that fact. You

do not need to list them again here.

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

5.4 Are there any agreements concerning the security and privacy of the data once it is shared? 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 What type of training is required for users from agencies outside the Department prior to receiving access to the information?

5.6 Are there any provisions in place for auditing the recipients' use of the information?

5.7 *Privacy Impact Analysis*: Given the external sharing, what privacy risks were identified and how were they 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 that 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 opportunity to consent to uses of said information, and the opportunity to decline to provide information.

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

6.1.1 If yes, identify the form of such notice. Was there a posted privacy policy, a Privacy Act notice on forms, or a System of Records Notice published in the Federal Register? If so, please provide copies or citations of such. If no form of notice was provided, explain why not.

6.1.2 Was the person aware that his or her information was being collected?

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

6.2.1 Can the person from or about whom information is collected decline to provide the information and if so, is there any penalty or denial of service that is the consequence of declining to provide the information?

6.3 Do individuals have an opportunity to consent to particular uses of the information? If such an opportunity exists, what is the procedure by which an individual would provide such consent?

6.4 *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 or if notice is not provided, what was the basis for this decision.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her

7.1 What are the procedures that allow individuals the opportunity to seek access to or redress of their own information?

7.1.1 Cite any procedures or regulations (other than the Department's FOIA/Privacy Act regulations) that your component has in place that allow an individual to seek access to or amendment of his/her information. For example, if your component has a customer service or outreach 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 or amendment provisions of the Privacy Act, explain the basis for the exemption or cite the regulation implementing the exemption.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

7.3.1 Are there other agency procedures that can be utilized by the individual with respect to this information?

7.4 *Privacy Impact Analysis*: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

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.

8.2 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 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?

8.6 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?

8.9 *Privacy Impact Analysis*: Given the access and security controls, what privacy risks were identified and how they were 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, or technology based on privacy risks and mitigation strategies.

Approval Process and Signature Page

After the component has prepared the PIA, approval shall be as follows:

a. PIAs for Major Information Systems (MIS)[3], as defined by OMB Memorandum M-03-22 and OMB Circular A-130, (MIS PIAs) and non-MIS systems are subject to Department review and approval by the DOJ Chief Privacy and Civil Liberties Officer.

b. While the E-Government Act PIA requirements do not apply to National Security Systems, it is Department policy to conduct internal PIAs for National Security Systems under this paragraph. Internal PIAs for National Security Systems are not subject to publication and will not be forwarded to OMB, but are otherwise subject to the process set forth in this paragraph.

c. Responsibilities

(1) The DOJ CIO shall:

(a) Provide guidance to all components on the preparation of PIAs, including an education and training program for components regarding their PIA responsibilities.

(b) Ensure compliance with the E-Government Act, OMB policy and this Order by

1 Using the Department's ITIM process (see Chapter 2, Section 5 of this Order and ITIM guidance documents);

[3] *Major information system* - embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.

2 Conducting periodic audits of component PIAs; and

3 Providing the Director of OMB with a copy of the PIA for each system for which funding is requested, as required by the E-Government Act. (Internal PIAs for National Security Systems will not be forwarded to OMB.)

(c) Maintain a current inventory of all PIAs approved by the Department and its components.

(d) For all MIS PIAs and non-MIS PIAs for all components other than FBI, DEA, USMS, ATF, EOIR, OJP, EOUSA and EOUST:

1 Conduct a technical review of the PIA, taking into consideration all relevant factors, including any component recommendations and whether or not the proposed system or system changes pose(s) an undue risk to privacy given the safeguards incorporated into the system, and the alternatives considered.

2 Consult with JMD Office of General Counsel (OGC) to identify legal issues and ensure compliance with the eGovernment Act, the Privacy Act, and other applicable statutes and regulations.

3 Make a recommendation of approval or disapproval to the DOJ Chief Privacy and Civil Liberties Officer.

a If the DOJ CIO recommends disapproval of a PIA, he shall identify the reasons for the recommendation and propose to the DOJ Chief Privacy and Civil Liberties Officer specific instruction on what changes are needed to achieve Departmental approval and the steps the component should take to resubmit the revised PIA for Department review.

b If the DOJ CIO recommends approval of a PIA, include a recommendation regarding publication of the PIA.

(2) The DOJ Chief Privacy and Civil Liberties Officer shall:

(a) Review all PIAs.

(b) Approve or disapprove the PIA taking into consideration the recommendation of the DOJ CIO and/or the Senior Component Official for Privacy and all relevant factors, including whether or not the proposed system, or system changes, pose(s) an undue risk to privacy given the safeguards incorporated into the system, and the alternatives considered.

(c) If the PIA is disapproved, provide the affected component with the reason(s) for disapproval and instruction on what changes are needed to achieve approval and the steps the component shall take to resubmit the revised PIA for Department review.

(d) If the PIA is approved, sign the PIA, and consult with the affected component to determine whether the PIA should be published. If the PIA is to be published, the component shall work with its FOIA office to make sure any relevant redactions are made before publication.

(3) The Component Heads shall:

(a) Ensure that PIAs are conducted in accordance with the E-Government Act of 2002, this policy, and applicable DOJ and OMB guidance, including OMB Memorandum M-03-22.

(b) Ensure that PIAs are conducted and reviewed prior to the development of a new system (or system modification), ideally when requirements are being analyzed and decisions are being made about data usage and system design.

(c) Ensure that PIAs are published in accordance with the requirements of the E-Government Act of 2002 and OMB guidance, including OMB Memorandum M-03-22. PIAs should be published on a publicly available web site on a page devoted to privacy or to the system for which the PIA was conducted, or if neither of these exists, in the component's FOIA electronic reading room. Only if a component is not able to publish the PIA on one of these web pages, should the PIA be published in the Federal Register.

(4) With respect to the FBI, DEA, USMS, ATF, EOIR, OJP, EOUSA and EOUST, the Senior Component Official for Privacy shall:

(a) Ensure that the Component IT Security Officer and the Component Legal Counsel are involved in the review or consulted before a PIA is recommended for approval.

(e) For non-MIS PIAs, either disapprove the PIA or forward the PIA to the PCLO for review with a recommendation for approval of the PIA and a recommendation as to whether the PIA should be published.

(f) For MIS PIAs, either disapprove the PIA or forward the PIA to the Department OCIO for review with a recommendation for approval of the PIA and a recommendation as to whether the PIA should be published.

Questions? Contact Us.

Privacy and Civil Liberties Office

U.S. Department of Justice Washington, D.C.

Email: [ ] Phone: [ ] Web Site Link: [ ]

Appendix I PIA Triggers

After completing a Privacy Threshold Analysis, please consult with your component's senior component official for privacy or the PCLO 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.