April 2010

United States Office of Personnel Management

Privacy Impact Assessment (PIA) Guide

This document implements the OPM Information Security and Privacy Policy

Chief Information Officer (CIO)

A New Day for the Civil Service

Table of Contents

REVISION HISTORY

Version Number	Version Date	Summary of Changes
1.1	April 2005	Initial Release
1.2	August 2005	Revised Draft Release
1.3	December 2005	Revised Draft Release
1.4	May 2006	Revised Draft Release
2.0	April 2010	Document revised in its entirety

EXECUTIVE SUMMARY

A privacy impact assessment (PIA) is one of the most important instruments through which the Office of Personnel Management (OPM) establishes public trust in its operations. The Chief Information Officer is responsible for ensuring that technologies developed and used by the agency 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 information technology (IT) system. The transparency and analysis of privacy issues provided by a PIA demonstrate that OPM actively engages system owners on the mitigation of potential privacy risks.

By conducting privacy threshold analyses (PTAs) and PIAs in accordance with the policies and procedures outlined in this PIA Guide, OPM demonstrates its consideration of privacy during the development of programs and IT systems and thus upholds the agency's commitment to maintain public trust and accountability. Without the trust of the public, the agency's mission is made more difficult. By documenting the procedures and measures through which the agency protects the privacy of individuals, the agency can better carry out its mission.

Therefore, PIAs serve several purposes:

- To evaluate the risk of collecting, maintaining, and disseminating information in identifiable form[1] on an OPM IT system.
- To evaluate the privacy and security protections on the IT system and ensure that the information is adequately protected.
- To ensure that information handling conforms to applicable legal, regulatory, and policy requirements throughout all stages of an IT system's development and operation.
- To allow the public to understand what information OPM collects and how it will be stored.

[1] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22.

- To assure the public that OPM is providing services in a manner that considers the sensitivity of the personal information it receives.

The version of this document that is posted to the Web is the official, authoritative version.

1. POLICY STATEMENT

It is OPM policy to ensure that all information technology (IT) systems that collect, maintain, or disseminate information in an identifiable form have a privacy impact assessment (PIA) or privacy threshold analysis (PTA) conducted by the system owner in compliance with the E-Government Act of 2002, Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) guidance.

2. INTRODUCTION

2.1 Purpose

The PIA Guide is designed to help OPM protect information about individuals that will be collected, maintained, or disseminated in identifiable form to meet the requirements of the E-Government Act of 2002, and related guidance. We recommend that anyone involved in the PTA and PIA process at OPM become familiar with these laws and guidance as outlined in section 2.3 below. In particular, this knowledge will help program offices conduct a privacy threshold analysis (PTA) and determine if a PIA must be completed.

A PIA is an analysis of how information is handled:

- To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.
- To determine the risks and effects of collecting, maintaining, and disseminating the information in an IT system.
- To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Because OPM handles a large volume of information that is subject to Privacy Impact Assessments, the agency must ensure that the appropriate practices and protections are in place and applied. This has become particularly important as developments in information technology (IT) have allowed information to be quickly and easily collected, as well as allowed OPM to provide quicker and more efficient services to the public.

2.2 Scope and Applicability

The PIA Guide and its references and appendices apply to all OPM information[2] and IT systems. OPM information includes data that is owned, sent, received, or processed by the agency and includes information in either physical or digital form. OPM IT systems include OPM hardware, software, and media.

Anyone who is involved in the PTA and PIA process at OPM must know and adhere to the procedures in the PIA Guide. The PIA Guide also applies to all contractors acting on behalf of

[2] The term "OPM information" is defined as information in either physical or digital form that is under the possession, custody, or control of OPM.

OPM and to non-OPM organizations or their representatives who are granted authorized access to OPM IT systems.

The PTA and PIA Templates are available from the Privacy Program Manager. We strongly recommend that you use the step-by-step tutorial in appendix A of this document to guide you when filling out a PTA, and the tutorial in appendix B when conducting a PIA.

If you are seeking information on OPM's privacy policies in general, please see the most recent version of the Information Security and Privacy Policy, available on the intranet at http://theo.opm.gov/policies/ispp/.

2.3 Legal Authority

OPM developed the PIA Guide to comply with the laws and guidance outlined below.

The E-Government Act of 2002[3]

The E-Government Act requires agencies to:

1. Conduct privacy impact assessments (PIAs).
2. Ensure that PIAs are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA).
3. Make PIAs available to the public via a public-facing Web site.
4. Report to OMB on the completion of PIAs.

Federal agencies must conduct a PIA **before** developing or procuring an IT system or project that collects, maintains, or disseminates information in identifiable form from or about members of the public. In addition, the E-Government Act requires that a PIA be completed before initiating, consistent with the Paperwork Reduction Act (PRA), a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies or employees of the Federal Government). This guidance applies to all OPM IT systems and electronic information collections in accordance with OMB guidance for implementing privacy provisions of the E-Government Act of 2002.

The E-Government Act stipulates that each PIA must address the following seven requirements:

1. What information is to be collected.
2. Why the information is being collected.
3. The intended routine use of the information.
4. With whom the information will be shared.
5. What notice or opportunities individuals have to decline to provide information.
6. How the information will be secured.
7. Whether a system of records is being created under the Privacy Act (5 U.S.C. 552a).

[3] E-Government Act is available at http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ347.107.pdf.

OMB Memorandum 03-22

OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of **personally identifiable information**. The guidance also requires Federal agencies to indicate within the PIA what opportunities individuals have to decline to provide information or to consent to particular uses of the information. Additionally, PIAs must identify what choices the agencies made regarding an IT system or electronic information collection as a result of performing the PIA. The OPM PIA Template asks a number of questions aimed at addressing these requirements.

This memorandum also states a PIA should be done only for IT systems that collect information on members of the public; however, OMB recommends conducting a PIA **on all IT systems that collect information in identifiable form, regardless of whom it is collected from.**

OMB Memorandum 05-08

OMB M-05-08, Designation of Senior Agency Officials for Privacy, establishes the Senior Agency Official for Privacy (SAOP) as having authority within the agency to consider information privacy policy issues at a national and agencywide level as well as having overall responsibility and accountability for:

1. Ensuring the agency’s implementation of information privacy protections, including the agency’s full compliance with Federal laws, regulations, and policies relating to information privacy, such as the Privacy Act.
2. Overseeing, coordinating, and facilitating the agency’s privacy compliance efforts.
3. Ensuring the agency’s employees and contractors receive appropriate training and education programs regarding the information privacy laws, regulations, policies, and procedures governing the agency’s handling of personal information.

In addition to this compliance role, the senior agency official must also have a central policy-making role in the agency’s development and evaluation of legislative, regulatory, and other policy proposals that have information privacy implications, including those relating to the agency’s collection, use, sharing, and disclosure of information in identifiable form.

At OPM, the Chief Information Officer (CIO) is designated as the Chief Privacy Officer (CPO) and the Senior Agency Official for Privacy (SAOP). In this role, the CIO reviews and signs all OPM PIAs. A PIA is not complete until the OPM CIO has signed it.

OMB Memorandum 07-16

OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, issued in 2007, requires agencies to eliminate the unnecessary use of social security numbers (SSNs). A PIA can be used as a tool to determine if adequate security and privacy controls are placed on a system to protect and prevent the breach of personally identifiable information (PII). OPM defines PII as information that:

1. Can be used to discern or trace a person's identity; and

2. Alone, or combined with other information, can be used to compromise the integrity of records relating to a person by permitting unauthorized access to or unauthorized disclosure of these records.

This means, for example, that a person's name alone would generally not constitute PII, but when linked to other identifying data such as the person's social security number, date of birth, or mother's maiden name, it would constitute PII. For more information on PII, please see the Privacy (PII) Web site on the OPM intranet.

2.4 Maintenance of the Official Version

The PIA Guide will be modified as appropriate to ensure it remains current with the following:

- Release of new executive, legislative, or technical policy or guidance.
- Changes in vulnerabilities, risks, or threats.
- OPM Inspector General (IG) findings stemming from audits.
- Changes to OPM's Information Security and Privacy Policy.

The OPM CIO reviews and approves all revisions to the PIA Guide. Once approved, a new version of the PIA Guide will be published on the OPM intranet.

3. PRIVACY IMPACT ASSESSMENT (PIA) POLICY AND PROCEDURES

3.1 When to Conduct a Privacy Threshold Analysis (PTA)

To determine if a privacy impact assessment (PIA) must be completed, it is OPM's policy that system owners must first complete a privacy threshold analysis (PTA). A properly completed and approved PTA provides documentation indicating that the system owner has accurately assessed whether or not a PIA is required, and is an effective tool for analyzing and recording the potential privacy documentation requirements of agency and program activities. As recommended in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122,[4] *"PTAs are used to determine if a system contains PII, whether a Privacy Impact Assessment is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system. PTAs should be submitted to an organization's privacy office for review and approval. PTAs are often comprised of simple questionnaires that are completed by the system owner. PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the information security officer, and the information officer."*

[4] NIST SP 800-122 is available at http://csrc.nist.gov/publications/PubsSPs.html.

All OPM IT systems must have a PTA. If the PTA reveals that the system collects no information in identifiable form, for example, the Privacy Program Manager will indicate in the PTA review that no PIA is required. The PTA must be incorporated into the system's certification and accreditation (C&A) package.

If, however, the PTA indicates that a PIA must be conducted on the system, most likely because the system collects, uses, or stores information in identifiable form, then the Privacy Program Manager reviews the PTA and provides further instructions to the system owner on conducting a PIA. Once a PIA is completed, it will document that the system owner has fulfilled the requirements of the E-Government Act of 2002, and the PIA will be incorporated into the C&A package and be posted on the OPM Web site.

Federal Information Security Management Act (FISMA) reporting requires system owners to review their PIAs every year and document whether there are any changes to the system. If there are changes, the corresponding PTA will identify whether or not the IT system requires an updated PIA.

3.2 When to Conduct a Privacy Impact Assessment (PIA)

A PIA must be conducted under the following circumstances:

- When a PTA indicates that a PIA is required.
- **Before** developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form.
- When a significant change occurs to a system.
- Every 3 years for existing systems without changes.

When a significant change occurs to a system, the system's PIA must be updated to reflect how the changes may affect the information. As defined by OMB Memorandum 03-22, significant changes include:

- **Conversions:** Converting paper-based methods to electronic systems, consistent with the Paperwork Reduction Act.
- **Anonymous to Nonanonymous:** Applying functions to an existing electronic information collection that changes 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 the process of managing information in identifiable form in the system.
- **Significant Merging:** Adopting or altering business processes so that Government databases holding information in identifiable form are merged, centralized, matched with other databases, or otherwise significantly manipulated.

- **New Public Access:** Applying user-authenticating technology (e.g., password, digital certificate, biometric) to an IT system that can be accessed by the public.
- **Commercial Sources:** Integrating information in identifiable form obtained from commercial or public sources into an existing information system database.
- **New Interagency Uses:** When agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form.
- **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 information in identifiable form.
- **Alteration in Character of Data:** When new information in identifiable form added to an electronic information collection raises the risks to personal privacy, such as the addition of health or privacy information.

It is important to note that systems that require a PIA may also require a system of records notice (SORN) or an information collection request (ICR), as outlined in sections 3.3 and 3.4 below.

3.3 When to Complete a System of Records Notice (SORN)

When conducting a PIA, the system owner may observe that information is being collected, used, and stored by their system and retrieved by a personal identifier to make determinations about members of the public to provide services to them. This may signal that the IT system is subject to the Privacy Act.

Among other requirements, the Privacy Act of 1974 requires agencies to complete a system of records notice (SORN) for systems that maintain, collect, use, or disseminate information about individuals **and** use an personal identifier – such as an ID number, social security number, date of birth, or other element – to retrieve the information being collected. Therefore, the Privacy Act SORN requirement is triggered by the collection information *that is actually retrieved by a personal identifier*.

It is important to note that completing a PIA does **not** fulfill the Privacy Act requirement to complete a SORN:

- A **PIA** is used to analyze the impact of the technology **that is using information in identifiable form.**

- A **SORN** is used to provide **notice to members of the public** that their information is being used by the agency.

See OPM System of Records Notice (SORN) Guide for details on OPM's SORN policies and procedures.

3.4 When to Complete an Information Collection Request (ICR)

Under the Paperwork Reduction Act (PRA), agencies must submit an information collection request (**ICR**) and obtain an Office of Management and Budget (OMB) electronic information collection approval number (also known as an OMB control number) for an information system *before using that system to collect information from members of the public numbering 10 or more, whether or not the information is considered to be information in identifiable form.* An ICR is submitted to OMB for approval of an electronic collection of information. However, before developing the ICR, a PIA must be conducted in accordance with the E-Government Act of 2002.

See OPM Paperwork Reduction Act Guide for detailed information on ICRs.

3.5 The PTA and PIA Process at OPM

This section details the steps for completing a PTA, and conducting a PIA if necessary.

Please see appendices A and B for step-by-step tutorials to guide you as you answer the questions on the PTA and PIA Templates.

3.5.1 The PTA Process

Step 1: The system owner completes a PTA and submits it to the Privacy Program Manager for review via the OPM PIA mailbox at PIAmail@opm.gov.

Step 2: The Privacy Program Manager does an initial review of the PTA for completeness and accuracy.

Step 3: If the PTA does not indicate a need for a PIA, the Privacy Program Manager notifies the system owner that no further action is needed. The Privacy Program Manager provides a copy of the PTA to the system owner and the OPM IT Security Officer (ITSO) for incorporation into the system's C&A package. If the PTA indicates a PIA is needed, the Privacy Program Manager provides a copy of the PTA to the system owner and the OPM IT Security Officer (ITSO) for incorporation into the system's C&A package and the system owner then completes the PIA process.

3.5.2 The PIA Process

Step 1: If a PIA is necessary, the system owner completes the PIA and submits it to the Privacy Program Manager at PIAmail@opm.gov. The Privacy Program Manager reviews the PIA and coordinates changes with the system owner if necessary.

Step 2: Once the system owner makes the appropriate changes, and the Privacy Program Manager requires no further changes, the system owner signs the PIA and returns it to the Privacy Program Manager.

Step 3: The Privacy Program Manager reviews the final version of the PIA and recommends that the PIA be reviewed and signed by the OPM CIO.

Step 4: Once the CIO signs the PIA, it is approved and complete. The Privacy Program Manager scans the final signed copy and provides it to the system owner and the ITSO for recordkeeping purposes and incorporation into the system's C&A package.

Step 5: The Privacy Program Manager submits the final PIA to the Office of Communications and Public Liaison (OCPL) for publication to the OPM PIA Internet site at https://www.opm.gov/privacy/pia.asp.

4. COMPLIANCE, ENFORCEMENT, AND EXCEPTIONS

Compliance with the PIA Guide is mandatory. Enforcement and monitoring of this policy is the responsibility of the Chief Information Officer (CIO). The CIO continually reviews and monitors the status of OPM's PIAs by monitoring:

- The effectiveness of the PIA process.
- Compliance with existing policies, procedures, standards, and guidelines.
- User awareness of PIAs.
- Active adoption of the PIA Guide requirements.

The OPM Office of the Inspector General (OIG) conducts independent audits to examine and evaluate OPM's compliance with the PIA Guide. The OIG provides the results to the CIO. The CIO submits the results of these audits in an annual report to OMB outlining OPM's PIA status and ongoing activities. Violations of the policy contained in the PIA Guide may result in the loss or limitation of access to OPM information systems and information. Anyone who violates the policy also may face administrative action ranging from counseling to removal from the agency, as well as criminal penalties or financial liability, depending on the severity of the misuse.

In addition, all OPM employees and contractors are subject to penalties established by the Privacy Act of 1974. Certain penalties apply to the misuse or unauthorized disclosure of personally identifiable information. The Act (5 U.S.C. 552a(g)) provides for civil remedies for injured parties, including actual damages, attorney fees, and litigation costs.

A policy violation is an **infringement or nonobservance of OPM policy**. If you suspect a policy violation, OPM employees must report it to their OPM supervisor, manager, associate director, or office director, as appropriate. Contractors must report suspected violations to their contracting officer's technical representative. The following preemptive actions must be taken to isolate the suspected violators and systems to prevent additional risk to OPM:

- The suspected violator's group lead must notify the OPM Center for Human Capital Management Services for additional guidance.
- The group lead is responsible for any disciplinary actions, in coordination with the Center for Human Capital Management Services and union representatives.
- The CIO is responsible for any technical actions.
- The CIO may restrict access to OPM information systems until the violator proves, to the satisfaction of the CIO, that the issue is resolved and there is no future risk.

The only exception to conducting a PIA is the completion of a PTA that indicates no PIA is necessary.

5. ROLES AND RESPONSIBILITIES

The roles identified in this section are directly responsible for the development and completion of PTAs and PIAs at OPM. Coordination among these roles is essential for the successful completion of a PIA.

5.1 Chief Information Officer (CIO)

Under OMB Memorandum 05-08, the Senior Agency Official for Privacy (SAOP) has special responsibilities to reinforce the Federal Government's mission to protect personal information. Under the Consolidated Appropriations Act of 2005, the Chief Privacy Officer (CPO) has similar responsibilities. At OPM, the CIO is the designated SAOP and CPO and provides the program infrastructure for completing PIAs. The CIO's responsibilities include:

- Designating responsibility for oversight of the PTA and PIA process as needed to the Privacy Program Manager.
- Reviewing and approving completed PIAs.
- Approving OPM's submission of the Privacy Management portion of the quarterly and annual Federal Information Security Management Act (FISMA) report to the OPM Inspector General (IG), which includes information on the current status of OPM PIAs.

5.2 Privacy Program Manager

The Privacy Program Manager is responsible for:

- Establishing and maintaining a methodology for conducting OPM PTAs and PIAs.
- Reviewing PTAs and PIAs for completeness and accuracy, and recommending approval of the PIA to the OPM CIO.
- Developing and recommending to the OPM CIO policies and procedures for the development of OPM PIAs.
- Ensuring that PIAs signed by the CIO are accurately posted to the OPM Web site.
- Coordinating the review and completion of FISMA annual and quarterly reports for PIAs.
- Coordinating with the Information Technology Security Officer (ITSO), or similar designated role, to ensure that PIAs or PTAs are included in a system's certification and accreditation (C&A) package.

5.3 Privacy Act Officer

The Privacy Act Officer is responsible for:

- Reviewing and supporting the development of the PTA and PIA by the system owner as necessary.
- Keeping an up-to-date inventory of all OPM PIAs.
- Assisting in the completion of FISMA annual and quarterly reports for PIAs.

5.4 Information Technology Security Officer (ITSO)

The Information Technology Security Officer (ITSO) is responsible for ensuring that OPM IT systems develop and maintain a complete C&A. A PTA or PIA must be part of the system's C&A package.

5.5 System Owner

A system owner is typically a senior program manager or executive responsible for a set of mission-critical functions of the agency. In this role, he or she serves as the person responsible for one or more IT supporting his or her assigned functions. The system owner may delegate completion of the PTA and PIA to the DSO; however, the system owner is ultimately responsible for the security and privacy of an IT system.

.

The system owner is responsible for:

- Completing a PTA for each system, and conducting the PIA if required.
- Ensuring that PTAs or PIAs are conducted on all systems before implementation or enhancement as required by OMB M-03-22 and OPM policy throughout the system's life cycle.
- Determining if significant changes are being planned or developed for an existing IT system or electronic information collection, requiring the completion of a PIA.
- Allocating proper resources to permit identification and remediation of privacy weaknesses identified on PIAs.
- Participating in PIA completion to validate all answers for the Privacy Program Manager's review.
- Signing and submitting completed PTAs and PIAs to the OPM PIA mailbox at PIAmail@opm.gov.
- Complying with all relevant Privacy Act requirements regarding any system of records, including, but not limited to, providing individuals with procedures for access and amendment of records.

5.6 Designated Security Officer (DSO)

The designated security officer (DSO) is appointed by an OPM associate director or office director to represent the interests of the program office in carrying out the security functions of the organization. As a representative of the program office, the responsibilities of the DSO may include:

- Working closely with the IT Security Officer (ITSO) and appropriate staff in the program offices to review, evaluate, and recommend appropriate information security and privacy measures and safeguards to protect information resources from loss; theft; misuse; unauthorized access, destruction, or use; and unauthorized modification, disclosure, or duplication, whether accidental or intentional..

- Assisting the system owner and Privacy Program Manager, when necessary, to complete PTAs and PIAs.

5.7 OPM Records Officer

The OPM Records Officer, who reports to the CIO, is responsible for collaborating with the system owner to develop an approved records schedule with the National Archives and Records Administration (NARA).

APPENDIX A: HOW TO FILL OUT A PRIVACY THRESHOLD ANALYSIS (PTA)

Before completing a privacy impact assessment (PIA) for a system or program, the system owner must first do a privacy threshold analysis (PTA) using the PTA Template available from the Privacy Program Manager. Once completed, submit it to the Privacy Program Manager at PIAmail@opm.gov in accordance with the procedures detailed in the PIA Guide. Please follow this tutorial for explanations on how to complete a PTA.

Please note: Do not use this appendix as a PTA template.

Tutorial

The responses to the questions on the PTA are intended to be short yet specific, so that the OPM Privacy Program Manager and Chief Information Officer can accurately assess whether a PIA is necessary. For the purposes of this tutorial, the bolded text below represents questions and statements that must be answered in the PTA Template.

Date submitted for review: Enter the date you submit the PTA to the Privacy Program Manager, using MM/DD/YYYY format.

Name of IT system: Enter the full name of the IT system.

What is the Unique Project Identifier (UPI) of the IT system: If you are required to complete a Capital Asset Plan (CAP) for this system, insert the UPI. If this is not applicable, enter N/A.

Name of Program Office: Enter the full name of the program office.

Name of IT system owner: Enter the name of the IT system owner.

Email for IT system owner: Enter the email address of the IT system owner.

Name of Designated Security Officer (DSO): Enter the name of the DSO.

Email for Designated Security Officer: Enter the email address of the DSO.

SPECIFIC QUESTIONS

1. **Status of IT system:** Insert a check mark next to the correct status of the system.

__This is a new IT system.

__This IT system has an existing PIA and as part of our yearly C&A review, we certify that there are no changes.

Date IT system first developed: MM/DD/YYYY

__This is an existing IT system that has been updated.

Date updated: MM/DD/YYYY

Please provide a general description of the update and what specifically has changed.

2. **Describe the IT system and its purpose:** Provide a general description of the IT system and its purpose in a way that a nontechnical person can understand.

3. **Indicate the stage of the IT system development life cycle the IT system is in.**

__Planning

__Development

__Production

4. **Do you collect, process, or retain information on (please check all that apply):**

__OPM employees

__Contractors working on behalf of OPM

__The public

5. **Do you use or collect social security numbers (SSNs)?**

__No.

__Yes. Why does the program collect SSNs? Provide the function of the SSN and the legal authority to do so.

6. **What information about individuals is collected, generated, or retained?** Provide a specific description of information that might be collected, generated, or retained, such as names, addresses, emails, etc.

7. **Does the IT system connect, receive, or share information in identifiable form or personally identifiable information (PII) with any other IT systems?**

__No.

__Yes. Please list any other IT systems that share this type of information with your IT system.

8. **Is there a Certification and Accreditation (C&A) record within OCIO's FISMA tracking system?**

__Unknown.

__No.

__Yes. Please indicate the determinations for each of the following:

Confidentiality: __Low __Moderate __High __Undefined

Integrity: __Low __Moderate __High __Undefined

Availability: __Low __Moderate __High __Undefined

PRIVACY THRESHOLD REVIEW

(To be completed by the OPM Privacy Program Manager)

Date reviewed by the OPM Privacy Program Manager: MM/DD/YYYY

DESIGNATION

__This is NOT a privacy sensitive IT system. The IT system contains no personally identifiable information and no PIA is required.

__PTA is sufficient at this time

__This IS a privacy sensitive IT system.

__A PIA is required

OPM PRIVACY PROGRAM MANAGER REVIEW COMMENTS

APPENDIX B: HOW TO FILL OUT A PRIVACY IMPACT ASSESSMENT (PIA)

If your completed privacy threshold analysis (PTA) indicates that a PIA is required for your system, please follow this tutorial for explanations, recommendations, and suggestions on how to complete the PIA. The responses to the questions on the PIA are intended to be detailed, so that the OPM Privacy Program Manager and Chief Privacy Officer can accurately assess potential privacy risks and effects of collecting, maintaining, and disseminating information in identifiable form or personally identifiable information.

Please note: Do not use this appendix as a PIA template. Please request the PIA Template from the Privacy Program Manager. Once completed, submit it to the Privacy Program Manager at PIAmail@opm.gov in accordance with the procedures detailed in the PIA Guide.

Tutorial

The abstract and overview sections of the PIA seek to collect information about the IT system to determine whether adequate privacy protections are associated with the information it collects, uses, or stores. For the purposes of this tutorial, the bolded text below represents questions and statements that must be answered in the PIA Template.

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- The first sentence should indicate the name of the program office and IT system.
- The second sentence should be a brief description of the IT system and its function.
- The third sentence should explain why the PIA is being conducted.

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 in the PIA. The overview should contain the following elements:

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- A general description of the information in the IT system.
- A description of a typical transaction conducted on the IT system.
- Any information sharing conducted by the IT system.
- A general description of the modules and subsystems, where relevant, and their functions.

- A citation of the legal authority to operate the IT system.

Section 1. Characterization of the Information

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

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

- Identify and list all information in identifiable form 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, email 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 identifier, photographic facial image, or any other unique identifying number or characteristic.

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

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

1.2 What are the sources of the information in the system?

- 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?

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

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

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

- Include a statement of why the particular information in identifiable form is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

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

1.4 How is the information collected?

- 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 or other technology used in the storage or transmission of information in identifiable form?

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

1.5 How will the information be checked for accuracy?

- 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.

- 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 agreements defined the collection of information?

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

Section 2. 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 how the information in the system will be used in support of the program's business purpose.

- Identify and list each use (both internal and external to OPM) of the information collected or maintained.

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

- Many systems sift through large amounts of information in response to a 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. Describe any type of analysis the system conducts and the data that is created from the analysis.

- 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.

- 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, explain why and how it is used.

This response should explain the following:

- If commercial data or publicly available data (open source) is directly or indirectly used, provide information on those uses in this section.

- If a program, system, or individual analyst uses commercial data or publicly available data, provide information on it here.

- If commercial data or publicly available data is used to verify information already maintained by OPM, provide information on it here.

- If new information previously not maintained by OPM is brought from an outside source, whether commercial or not, provide information on it here.

Section 3. Retention of Information

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

3.1 What information is retained?

- Identify and list all information collected from question 1.1 that is retained by the system.

3.2 How long is information retained?

- In some cases OPM may choose to retain files in active status and archive them after a certain period of time. State active file retention periods as well as archived records, in number of years, as well as the General Records Schedule. The OPM records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. See the OPM Records Management Handbook located at http://theo.opm.gov/References/IT/policies.asp

3.3 Has the retention schedule been approved by the OPM records officer and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

- An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The OPM records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the OPM records officer will notify the system owner. See the OPM Records Management Handbook located at http://theo.opm.gov/References/IT/policies.asp for additional information on retention schedules.

Section 4. Internal Sharing and Disclosure

The following questions are intended to define the scope of information sharing within OPM.

4.1 With which internal organizations is information shared? What information is shared, and for what purpose?

- The term "internal" means program offices, contractor-supported IT systems, and any other organization or IT system within OPM. This question is directed at the sharing of information internally within OPM.

- Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within OPM with which information is shared.

- State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

- For each interface with a system outside your program office, state what specific information is shared with the specific program office, contractor-supported IT system, and any other organization or IT system within OPM.

4.2 How is the information transmitted or disclosed?

- Describe how the information is transmitted to each program office, contractor-supported IT system, and other organization or IT system listed in question 4.1.

- For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

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

Section 5. External Sharing and Disclosure

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

5.1 With which external organizations is information shared? What information is shared, and for what purpose?

- The term "external" means other departments, agencies, and organizations that are not part of OPM. This could be other departments, law enforcement and intelligence agencies, the private sector, and State and local entities. This question is directed at sharing information with other agencies, as well as with private entity and State or local governments.

- Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

- If a system of records notice (SORN) has been published for the system, summarize the most relevant routine uses. For example, if the system provides full access to another agency for their use of the information, 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 this summary would be that the system does not regularly handle requests from Congressional members.

- For each interface with a system outside OPM, state what specific information is shared with each specific partner.

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

5.2 Is the sharing of information outside the agency compatible with the original collection?

- What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party?

5.2.1 If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of OPM.

- Indicate the name of the SORN and briefly describe the routine use from the applicable SORN.

- If a 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 agency and what security measures safeguard its transmission?

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

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

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

- Any sharing conducted per a routine use in the applicable SORN should be transmitted in a secure manner. Additionally, if information is shared under an MOU, memorandum of agreement (MOA), or similar formal agreement, describe whether and how the agreement requires secured transmission and storage of shared data.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

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

- This question is directed at the notice provided before 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, provide the citation.

- If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

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

- The issue of notice, particularly notice found in a SORN, involves the advice of counsel. Consult your assigned counsel on issues concerning the sufficiency of notice to the public on an information collection.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

- 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?

- 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 or her information. If specific consent is required, how would the individual consent to each use?

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

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

- Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the OPM FOIA Web page at http://www.opm.gov/efoia to obtain information about FOIA points of contact and information about agency FOIA processes.

- 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).

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

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

- Describe 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, state as much.

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

- How is an individual made aware of the procedures for correcting his or her information? This may be through notice at collection or 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 significantly weakened.

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

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

Section 8. 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?

- Describe the process by which an individual receives access to the system.

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

- 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 OPM contractors have access to the system?

- If so, 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?

- OPM offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

8.4 Has C&A been completed for the system?

- If so, provide the date the Authority to Operate (ATO) was granted. Please note that all systems containing PII are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

APPENDIX C: GLOSSARY

commercial aggregator: A firm that collates and presents information about an individual's bank accounts, investments, insurance policies, etc., via a single mechanism or Web site.

commercial data: Information accessed or obtained by a Government agency from a nongovernmental entity, including commercial and nonprofit enterprises.

confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3.)

information collection: The obtaining, causing to be obtained, soliciting, or requiring the disclosure to an agency, third parties or the public of information by or for an agency by means of identical questions posed to, or identical reporting, recordkeeping, or disclosure requirements imposed on, ten or more persons, whether such collection of information is mandatory, voluntary, or required to obtain or retain a benefit. (Source: 5 CFR 1320.3.)

information in identifiable form: Information in an IT system or online collection: (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. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Section 208(d) of the E-Government Act defines it as "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form." (Source: OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.)

information technology (IT) system: Any equipment, software, or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. (Source: Clinger-Cohen Act.)

integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. (Source: 44 U.S.C. 3542.)

major application (MA): Application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might include many individual application programs and hardware, software, and telecommunications components. MAs can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function. (Source: NIST SP 800-18.)

Note: All Federal applications require some level of protection. However, certain applications, because of the information in them, require special management oversight and must be treated as a major application. Adequate security for other applications must be provided by security of the systems in which they operate. (Source: OMB Circular A-130, (A) (2) (d).)

non-major application: Any initiative or investment not meeting the definition of a major application defined above but is part of the agency's IT portfolio. (Source: OMB Circular A-11, Section 53.4.)

personally identifiable information (PII): OPM’s definition: information that can be used to discern or trace a person’s identity; and alone, or combined with other information, can be used to compromise the integrity of records relating to a person by permitting unauthorized access to or unauthorized disclosure of these records. This is different from “information in identifiable form” as referred to in the E-Government Act of 2002.

physical security controls: Measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. These safeguards might include protections against fire, structural collapse, plumbing leaks, physical access controls, and controls against the intercept of data. (Source: NIST SP 800-12.)

publicly available data: Data taken from public Web sites or any other publicly available source.

privacy impact assessment (PIA): Analysis of how information is handled to:

1. Ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy.
2. Determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system.
3. Examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

(Source: OMB Memorandum 03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003.)

privacy threshold analysis (PTA): Methodology that provides information technology (IT) security professionals with a process for assessing whether a PIA is necessary.

record: Any item, collection, or grouping of information about individuals that is maintained by an agency, including, but not limited to, their education, financial transactions, or medical, criminal, or employment history and that contains their name; or that contains the identifying number, symbol, or other identifying information assigned to the individual, such as a fingerprint, voiceprint, or photograph. (Source: 5 U.S.C. 552a(a)(4).)

routine use: Use of a record for a purpose that is compatible with the purpose for which it was collected.

significant change: Any change that is made to the system environment or operation of the system. The following are examples of significant changes as defined by OMB M-03-22:

- Conversion
- Anonymous to nonanonymous
- Significant system management changes
- Significant merging
- New public access
- Commercial sources
- New interagency uses
- Internal flow or collection
- Alteration in character of data

system of records: Group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. (Source: 5 U.S.C. 552a(a)(5).)

system of records notice (SORN): Notice that must be published in the Federal Register for all systems that collect information in identifiable form on individuals and use a personal identifier, such as an ID number, social security number, date of birth, or other element, to retrieve the individuals record. The SORN informs the public what information is contained in the system, how it is used, how individuals may gain access to information about themselves, and other specific aspects of the system. (Source: 5 U.S.C. 552a(e)(4).)

system owner: Typically a senior program manager or executive responsible for a set of mission-critical functions of the agency. In this role, he or she serves as the person responsible for one or more information system supporting his or her assigned functions. The system owner may delegate completion of the PTA and PIA to the designated security officer (DSO); however, the system owner is ultimately responsible for the security and privacy of an IT system.

APPENDIX D: ACRONYMS

C&A	certification and accreditation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CPO	Chief Privacy Officer
DSO	designated security officer
FISMA	Federal Information Security Management Act of 2002
FOIA	Freedom of Information Act of 1966
FR	Federal Register
IG	inspector general
IT	information technology
ITSO	Information Technology Security Officer
LAN	local area network
M	memorandum
MA	major application
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OCPL	Office of Communications and Public Liaison
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PDF	portable data format
PII	personally identifiable information
PIA	privacy impact assessment
PRA	Paperwork Reduction Act
PTA	privacy threshold analysis
SAOP	Senior Agency Official for Privacy
SOR	system of records
SORN	system of records notice
SSN	social security number
SP	Special Publication
URL	uniform resource locator
U.S.C.	United States Code

APPENDIX E: REFERENCES

- 44 U.S.C. 3542.
- Consolidated Appropriations Act, 2005, Pub. L. 108-447.
- E-Government Act of 2002.
- Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII**)**.
- OMB Memorandum M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
- OMB M-05-08, Designation of Senior Agency Officials for Privacy.
- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information.
- Privacy Act of 1974, as amended, 5 U.S.C. 552a, Pub .L. 93-579.

UNITED STATES
OFFICE OF PERSONNEL MANAGEMENT
Chief Information Officer (CIO)
1900 E Street, NW
Washington, DC 20415