

**DEPARTMENT OF THE INTERIOR  
Privacy Impact Assessment  
And Guide**



**Office of the Chief Information Officer**

**Version:9.16.02**

**The Department of the Interior  
Privacy Impact Assessment  
And Guide**

**Table of Contents**

Introduction	i – v
Privacy Impact Assessment Template	Section I (7 pages)
Privacy Impact Assessment Guide	Section II (14 pages)
Web Links to Privacy Policy Resources	Section III (4 pages)

# The Department of the Interior Privacy Impact Assessment And Guide

## INTRODUCTION

Section I of this document is the Department of the Interior's (DOI) Privacy Impact Assessment (PIA). Section II is a guide that provides information on completing many of the PIA questions. Section III provides web links to resources on the Privacy Act and Government privacy protection policy.

### **What is the Purpose of the PIA?**

The objective of the PIA is to assist DOI employees in identifying and addressing information privacy when planning, developing, implementing, and operating individual agency information management systems. The PIA will help DOI employees consider and evaluate whether existing statutory requirements and key information management concepts and requirements are being applied to new and modified systems that contain personal information. These requirements are drawn from the Privacy Act, Computer Security Act, the Clinger-Cohen Act, the Government Paperwork Reduction Act, the Freedom of Information Act, and Office of Management and Budget (OMB) Circulars A-130: Management of Federal Information Resources and A-123: Management Accountability.

The PIA is a new Government requirement to ensure that system owners and developers consider and evaluate existing statutory and key information management requirements that must be applied to new or modified Government systems that contain personal information. Going through the PIA process will also help to identify sensitive systems so that appropriate information assurance measures are in place, such as secured storage media, secured transmission and access controls.

The goals accomplished in completing a PIA include:

- Providing senior DOI management with the tools to make informed policy and system design or procurement decisions based on an understanding of privacy risk, and of options available for mitigating that risk;
- Ensuring accountability for privacy issues with system project managers and system owners;
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance with applicable privacy law and regulation, as well as accepted privacy policy; and
- Providing basic documentation on the flow of personal information within DOI systems for use and review by policy and program staff, systems analysts, and security analysts.

## **What is Personal Information?**

Personal information is information about an identifiable individual that may include but is not limited to:

- Information relating to race, national or ethnic origin, religion, age, marital or family status;
- Information relating to education, medical, psychiatric, psychological, criminal, financial, or employment history;
- Any identifying number, symbol or other particular assigned to the individual; and
- Name, address, telephone number, fingerprints, blood type, or DNA.

## **When is a PIA Required?**

Although the Internal Revenue Service's PIA was recommended by the Federal Chief Information Officer Council in February 2000 as a Government-wide "Best Practice" at [http://www.cio.gov/Documents/pia\\_for\\_it\\_irs\\_model.pdf](http://www.cio.gov/Documents/pia_for_it_irs_model.pdf), OMB now requires that a PIA be submitted with revised Exhibit 300s for budget requests (see OMB Circular A-11, sections 31.8, 53.1, and 300.9 at <http://www.whitehouse.gov/omb/circulars/a11/02toc.html>). Exhibit 300, Part I, Questions A. c. and E.5 and Part II C.5 now ask if a PIA or privacy risk assessment was performed for the project.

A completed PIA is also required for DOI Information Technology (IT) Security Certification and Accreditation (C&A). The DOI IT Security Plan outlines the policies and procedures for the C&A process.

If personally identifiable information is paired with geographic information and related spatial data, PIAs must be completed for these systems as well. The revised OMB Circular A-16 on "Coordination of Geographic Information and Related Spatial Data Activities" dated August 19, 2002 also requires that those agencies that collect, use, or disseminate geographic information and/or carry out related special data activities also comply with Government law and policy on privacy protection (see 2.a. and 8.a.7 of the Circular).

For new or modified systems, which do not require an Exhibit 300 or C&A, it is recommended that a PIA be used to ensure that measures are in place to protect privacy in all DOI information systems that contain personal information.

## **Suppose the System I am Evaluating has No Personal Information in it?**

If the system is being evaluated for an Exhibit 300 and an IT Security C&A, and it is found that the system contains no personal information identifiable to an individual such as that listed above, indicate after the appropriate question on the Exhibit 300 or C&A forms that a review of the data elements in the system was performed and there is no personal information in the system. Complete Sections A and B.1. of the PIA and provide it with the Exhibit 300 and the IT Security C&A package to address who performed the data review and what the results were for future reference if needed by OMB, the IT Security Manager or Privacy Act Officer.

**Note:** In cases where systems are networks that house information systems and do not actually collect, manipulate, or use the data in the systems they house complete Sections A and B.1 of the PIA. Indicate what systems are managed by this network. A separate Privacy Assessment should be completed for each of those systems. Attach this analysis to the Exhibit 300 and IT Security Certification.

**Who Completes a PIA?**

Since the requirements of a PIA must be addressed at the early stages of system development, ideally the system owner and system developer will complete the assessment. System owners must address what data is to be used, how the data is to be used, and who will use the data. System developers and managers must be aware of privacy requirements when systems are conceptualized and designed. The system developers must address whether the implementation of the owner’s requirements presents any threats to privacy. The system owner and developer will need to coordinate certain responses with the bureau/office Privacy Act Officer, Information Collection Clearance Officer, IT Security Manager, Records Officer, and possibly CIO, if necessary.

**When Must a PIA be Completed?**

The requirements identified in the PIA ideally must be considered early when planning, developing, implementing, and modifying individual agency information management systems that contain personal information (this applies not only to Privacy Act systems of records where personal information is retrieved by the subject’s name or other identifier, but any system that contains personal information).

New and modified systems also include those created by extracting data from an existing system which alters the purpose for which the information is used; those created from combining data from two or more existing systems; and systems created from information collected from individuals off DOI web pages.

**What are the steps to complete a Privacy Impact Assessment?**

The chart below identifies some steps involved with completing a PIA.

<b>Steps</b>	<b>Who Does It</b>	<b>What is Done</b>
<b>1.</b>	Owner and Developer	Obtain a copy of the assessment from your bureau/office Privacy Act Officer or from the Department Privacy Act Officer or IT Portfolio Management Division, Office of the Chief Information Officer (CIO). Request briefings on Government and Interior privacy, security, records, and Freedom of Information Act requirements.
<b>2.</b>	Owner and Developer	Complete questions on the PIA, and consult with necessary parties (e.g. FOIA Officer, Data Administrator, Privacy Officer, IT Security Manager, Information Collection Clearance Officer).

3.	Owner, Developer, CIO, Privacy Officer, IT Security Officer	All parties should reach an agreement on design requirements and resolve any identified privacy or security risks. Ensure that all appropriate surnames are obtained.
4.	Bureau/Owner, IT Security Manager	Review PIA for IT Security C&A purposes. Provide completed PIA to the bureau/office IT Security Manager and bureau/office Privacy Act Officer, and provide copy with Capital Asset planning exhibit 300.

**Note:** Also allow time to coordinate information collection approvals if necessary through your office’s Information Collection Clearance Officer and the Office of Management and Budget (usually a 120 day process); Privacy Act system of records notices with your office’s Privacy Act Officer (usually a 120 day process); or Records Disposition Schedules with your office’s Records Officer.

**Where Can I Go for More Information?**

For assistance and to obtain an electronic version of this document, please contact your bureau/office Privacy Act Officer, the Departmental Privacy Act Officer or the Information Technology Portfolio Division in the Office of the Chief Information Officer (CIO), or refer to the DOI Privacy Program Homepage at <http://www.doi.gov/ocio/privacy/>.

## SECTION I

### **Department of the Interior Privacy Impact Assessment**

Once completed please provide copies of the PIA to the following:

- Bureau/office IT Security Manager (when a C&A is required)
- Bureau/office Privacy Act Officer
- Office of Management and Budget (OMB) Capital Planning Exhibit 300 Submission (when an Exhibit 300 is required).

Also refer to the signature approval page at the end of this document.

#### **A. CONTACT INFORMATION:**

- 1) **Who is the person completing this document?** (Name, title, organization and contact information).
  
- 2) **Who is the system owner?** (Name, organization and contact information).
  
- 3) **Who is the system manager for this system or application?** (Name, organization, and contact information).
  
- 4) **Who is the IT Security Manager who reviewed this document?** (Name, organization, and contact information).
  
- 5) **Who is the Bureau/Office Privacy Act Officer who reviewed this document?** (Name, organization, and contact information).

#### **B. SYSTEM APPLICATION/GENERAL INFORMATION:**

- 1) **Does this system contain any personal information about individuals?**

- 2) What is the purpose of the system/application?
  
- 3) What legal authority authorizes the purchase or development of this system/application?

**C. DATA in the SYSTEM:**

- 1) What categories of individuals are covered in the system?
  
- 2) What are the sources of the information in the system?
  - a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?
  
  - b. What Federal agencies are providing data for use in the system?
  
  - c. What Tribal, State and local agencies are providing data for use in the system?
  
  - d. From what other third party sources will data be collected?
  
  - e. What information will be collected from the employee and the public?
  
- 3) Accuracy, Timeliness, and Reliability
  - a. How will data collected from sources other than DOI records be verified for accuracy?

**b. How will data be checked for completeness?**

**c. Is the data current?** What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

**d. Are the data elements described in detail and documented?** If yes, what is the name of the document?

**D. ATTRIBUTES OF THE DATA:**

- 1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**
  
- 2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**
  
- 3) Will the new data be placed in the individual's record?**
  
- 4) Can the system make determinations about employees/public that would not be possible without the new data?**
  
- 5) How will the new data be verified for relevance and accuracy?**
  
- 6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

- 7) **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**
  
- 8) **How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**
  
- 9) **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

**E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:**

- 1) **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**
  
- 2) **What are the retention periods of data in this system?**
  
- 3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**
  
- 4) **Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**
  
- 5) **How does the use of this technology affect public/employee privacy?**

- 6) **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**
  
- 7) **What kinds of information are collected as a function of the monitoring of individuals?**
  
- 8) **What controls will be used to prevent unauthorized monitoring?**
  
- 9) **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**
  
- 10) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

**F. ACCESS TO DATA:**

- 1) **Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)
  
- 2) **How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?
  
- 3) **Will users have access to all data on the system or will the user's access be restricted? Explain.**
  
- 4) **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

- 5) **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?** If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?
  
- 6) **Do other systems share data or have access to the data in the system? If yes, explain.**
  
- 7) **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**
  
- 8) **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**
  
- 9) **How will the data be used by the other agency?**
  
- 10) **Who is responsible for assuring proper use of the data?**

**The Following Officials Have Approved this Document**

**1) System Manager**

\_\_\_\_\_ (Signature)

**Name**

**Title**

**2) IT Security Manager**

\_\_\_\_\_ (Signature)

**Name**

**Title**

**3) Privacy Act Officer**

\_\_\_\_\_ (Signature)

**Name**

**Title**

## SECTION II

### **Guidelines for the Department of the Interior Privacy Impact Assessment**

For assistance and to obtain an electronic version of this document, please contact your bureau/office Privacy Act Officer, the Departmental Privacy Act Officer or the Information Technology (IT) Portfolio Division in the Office of the Chief Information Officer (CIO), or refer to the DOI Privacy Program Homepage at <http://www.doi.gov/ocio/privacy/>.

After many of the questions below statutory, regulatory, and internal guidelines are identified for the user to assist in properly responding to the Privacy Impact Assessment (PIA) questions. Also included is information that will be useful in completing Exhibit 300s and Privacy Act system of records notices for the *Federal Register* and accompanying narrative statements when required.

In cases where systems are networks that house information systems and do not actually collect, manipulate, or use the data in the systems they house, and where systems are evaluated and no personally identifiable information is found, complete Sections A and B.1 of the PIA. Attach this analysis to the Exhibit 300 and IT Security Certification to verify that a review for personally identifiable information was made for the system.

**Note:** For the network systems above, indicate what systems are managed by this network. A separate Privacy Assessment should be completed for each of those systems.

#### **A. CONTACT INFORMATION:**

- 1) **Who is the person completing this document?** (Name, title, organization and contact information).
- 2) **Who is the system owner?** (Name, organization and contact information).

This is the official responsible for this system that will implement the legal information resources management requirements (privacy, security, Freedom of Information Act, records, data administration)? For more information on the responsibilities of a system owner refer to Departmental Manual 375 DM 13: Information Resources Management.

- 3) **Who is the system manager for this system or application?** (Name, organization, and contact information).

For system manager responsibilities identified by the Privacy Act, refer to the Department of the Interior (DOI) Privacy Act Manual Sections 383 DM 1.4.F., 3.6, and 4.4.C., and DOI Privacy Act regulations at 43 CFR 2.48, 2.51, 2.52, 2.56 and 2.57 - 2.77. The DOI Manual Section on IT at 376 DM 13: Automated Information Systems Management Accountability identifies the IT related responsibilities of a system manager.

- 4) **Who is the IT Security Manager who reviewed this document?** (Name, organization, and contact information).
  
- 5) **Who is the Bureau/Office Privacy Act Officer who reviewed this document?** (Name, organization, and contact information).

#### **B. SYSTEM APPLICATION/GENERAL INFORMATION:**

A system that collects, maintains, uses, and disseminates information **and** that can be retrieved by the name or other identifier particular to an individual(s) is a system of records (SOR) covered by the Privacy Act. For more information on SORs, refer to the Departmental Privacy Act regulations at 43 CFR 2.46 and DOI Privacy Act Manual Section 383 DM 1.4.

- 1) **Does this system contain any personal information about individuals?** (Versus statistical, geographic, or wildlife with no link to a name or identifier, for example).

**Note:** If personally identifiable information is paired with geographic information and related spacial data, PIAs must be completed for these systems as well. The revised OMB Circular A-16 on “Coordination of Geographic Information and Related Spacial Data Activities” dated August 19, 2002 also requires that those agencies that collect, use, or disseminate geographic information and/or carry out related special data activities also comply with Government law and policy on privacy protection (see 2.a. and 8.a.7 of the Circular).

Also refer to the Federal Geographic Data Committee “Privacy Principles” at Federal Geographic Data Committee Privacy Policy at <http://www.fgdc.gov/fgdc/policies/privacypolicy.pdf>

- 2) **What is the purpose of the system/application?**

What will be the primary uses of the system/application? How will this support the program’s mission?

**Narrative Statement Information:** This information is used when submitting a narrative statement to Office of Management and Budget (OMB) and Congress for new and major

amendments to Privacy Act systems of records (see 383 DM 5, Appendix 2, A.1.). It is also included in the Privacy Act system of records notice published in the *Federal Register* (see 383 DM, Appendix 3). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative and notice.

**3) What legal authority authorizes the purchase or development of this system/application?**

What are the statutory provisions or Executive Orders that authorize the maintenance of the information to meet an official program mission or goal?

Narrative Statement Information: This information is used when submitting a narrative statement to OMB and Congress for new and major amendments to Privacy Act systems of records (see 383 DM 5, Appendix 2, A.2.) and identifying the authority for the maintenance of the information in the Privacy Act notice (see 383 DM 5, Appendix 3). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative and notice.

**C. DATA in the SYSTEM:**

Responses to this section will be helpful in completing Exhibit 300, Part II, A. 7.

**1) What categories of individuals are covered in the system? (E.g., employees, contractors, visitors to National Parks, and volunteers)**

Narrative Statement Information: This information is used when submitting a narrative statement to OMB and Congress for new and major amendments to Privacy Act systems of records (see 383 DM 5, Appendix 2, A.1.a.). This information is also used in the notice (see 383 DM 5, Appendix 3). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative and notice.

**2) What are the sources of the information in the system?**

**a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?**

Examples of sources of the information include information that comes from individuals applying for permits, and forms individuals completed from a bureau web page.

This will be helpful in responding to Exhibit 300, Part II, B.4. It can also be used in preparing the Privacy Act system of records notice (see 383 DM 5, Appendix 3). If the

system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the notice.

**b. What Federal agencies are providing data for use in the system?**

Where does the data originate? (E.g., the Social Security Administration, U.S. Forest Service, Office of Personnel Management and Health and Human Services)

Narrative Statement Information: This information (and that in c. and d. below) is used when submitting a narrative (see 383 DM 5, Appendix 2, A.4.). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative.

**c. What Tribal, State and local agencies are providing data for use in the system?**

**d. From what other third party sources will data be collected?**

A third party is usually a non-Federal person or entity, who may be a source of data/information (i.e., an informant, an internet service provider, an organization).

**e. What information will be collected from the employee and the public?**

Be as specific as possible and list information on individuals collected from the public such as a social security number, address, debts owed and telephone numbers. Employee information may include badge number, user identifier, telephone number, social security number and health information.

If you are collecting information from the public, contact your Information Collection Clearance Officer to ensure that you have an OMB approval to do so or to determine whether you need to obtain an OMB approval to collect the information. The Paperwork Reduction Act of 1980 establishes requirements for collecting the same information from 10 or more individuals (this does not include employees acting in their official capacity). This information may be helpful in responding to Exhibit 300, Part II, D.3. regarding OMB approval codes for collections of information.

This information can also be used in preparing the Privacy Act system of records notice (see 383 DM 5, Appendix 3). If the system already has a Privacy Act system of records notice, then the information for this question should reflect the information already in the notice.

**3) Accuracy, Timeliness, and Reliability**

The Privacy Act of 1974 requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. These requirements are statutory and

need to be addressed. If the data does not meet any one of these four components, then fairness in making any determination is compromised.

There must be documentation as to how the requirements are enforced while the data is retained in the system, and what data is considered sensitive. Maintaining Meta Data (documentation on the data) is important so it can be referenced in the future to identify data conditions when making decisions about data from a system (see OMB Circular A-130 8.a.4, DOI Manual Section 383 DM 9.2 and 43 CFR 2.48(b)).

Although the following does not apply to information covered by the Privacy Act, information used to make or influence decisions and that is published in the public domain, may be subject to challenge by the public under the Data Quality Act. The need to publish correct and useful information should always be a concern. Third party information or information originating outside of the Department of the Interior that is adopted by DOI in any decision-making process is subject to the Data Quality Act.

**a. How will data collected from sources other than from DOI records be verified for accuracy?**

The information has to have some form of verification for accuracy due to the Privacy Act provisions that require that only relevant and accurate records should be collected and maintained about individuals.

Data accuracy and reliability are important requirements in implementing the Privacy Act. The statute requires that each agency that maintains a system of records shall “maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” (5 U.S.C. 552a(e)(5)).

**b. How will data be checked for completeness?**

The data must be complete before the data is deemed accurate.

**c. Is the data current?**

What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

If the data is out-of-date, then the relevancy and accuracy of the data are called into question. This is particularly true with data warehousing. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.

**d. Are the data elements described in detail and documented? If yes, what is the name of the document?**

The data element description should provide information on the legal requirements of the data. Data elements should also be documented in keeping with OMB Circular A-130 requirements for determining the privacy impact at each stage or phase of the information life cycle.

**D. ATTRIBUTES OF THE DATA:**

**1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

The Privacy Act at 5 U.S.C. 552a(e)(1) requires that "each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President." Refer to Departmental Regulations on the Privacy Act at 43 CFR 2.48: Standards for Maintenance of Records Subject to the Act.

Narrative Statement Information: This information is used when submitting a narrative statement (see 383 DM 5, Appendix 2, A.6.). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative.

**2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

All enhanced or modernized systems most likely will derive new data and create previously unavailable data about an individual through aggregation from the information collected.

What is meant by derived and aggregation?

□ □ Derived data is obtained from a source for one purpose and then the original information is used to deduce/infer a separate and distinct bit of information that is aggregated to form information that is usually different from the source information.

□ □ Aggregation of data is the taking of various data elements and then turning it into a composite of all the data to form another type of data. (For example, tables or data arrays).

Refer also to the General Accounting Office (GAO) report on "Data Linkage and Privacy" (GAO-01-126SP) at <http://www.gao.gov/new.items/d01126sp.pdf>.

Narrative Statement Information: This information is used when submitting a narrative statement (see 383 DM 5, Appendix 2, A. 3.). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative.

**3) Will the new data be placed in the individual's record?**

Will the new data that is created either by deriving or aggregating the data be placed in a new filing system? Or will it be placed in an existing file system with information on the individual (for example, in the employee's Official Personnel File or manager's file)?

**4) Can the system make determinations about employees/public that would not be possible without the new data?**

Narrative Statement Information: This information is used when submitting a narrative statement (see 383 DM 5, Appendix 2, A.3). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative.

**5) How will the new data be verified for relevance and accuracy?**

Refer to the information provided for question C. 3 above.

**6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls, if any, should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not accessed inappropriately or by someone unauthorized to access the data. These controls will help to prevent unauthorized use from occurring. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III. Another consideration is the use of Role Based Access Controls (RBAC). For more information on RBAC go to <http://csrc.nist.gov/rbac/>.

The DOI IT Security Plan (ITSP) describes the practice of identification and authentication that is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security C&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

Narrative Statement Information: Information from this question and (7), (8) and (9) below is used when submitting a narrative statement (see 383 DM 5, Appendix 2, A.5). This information can also be used in preparing the Privacy Act system of records notice (see 383 DM 5, Appendix 3). If the system already has a Privacy Act system of records notice, then the information for this question should reflect the information already in the narrative and notice.

**7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.**

The DOI IT Security Risk Assessment Guide outlines a process deliberately developed to be broad in scope, considering not only the technical security aspects but the managerial and operational as well. When processes are consolidated, management must maintain the proper controls minimizing the risk to all systems. The IT Security C&A process requires that a risk assessment be performed regularly on DOI's major applications, networks, and computer installations.

**8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.**

Data can be retrieved a number of ways, but there is usually a personal identifier associated with data retrieval mechanism. A system with data on individuals that is retrieved by a name or personal identifier is a Privacy Act system and will need a published system of records notice in the *Federal Register*. If you do not have a published system or record notice, contact your office's Privacy Act Officer. For a listing of DOI bureau/office Privacy Act Officers go to the DOI Privacy Program web page at <http://www.doi.gov/ocio/privacy/>.

**9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

**E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:**

**1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

**2) What are the retention periods of data in this system?**

The retention periods of data/records that the DOI manages are contained in either the General Records Schedule or the bureau/office Records Schedule(s). For the particular data being created/maintained in the system/application/process, these are the authoritative sources for this information. Your bureau/office Record Management Officer is another source for determining the retention period of data used by the agency. For a listing of the bureau/office Records Officers go to the DOI Records Management web site at <http://www.doi.gov/ocio/records/>.

**3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

Disposing of the data at the end of the retention period is the last state of life cycle management. Contact your bureau/office Records Management Officer for further assistance <http://www.doi.gov/ocio/records/>. Records subject to the Privacy Act have special disposal procedures. Refer to 383 DM 8.8 for instructions. Also refer to DOI IRM Bulletin No. 2001-004, Protecting Sensitive Data When Transferring, Donating, or Disposing of Computer Equipment at <http://www.doi.gov/ocio/bulletins/2001-004bul.htm>.

**4) Is the system using technologies in ways not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

**5) How does the use of this technology affect public/employee privacy?**

Depending on the technology being used, it may have little or no impact on either public or employee privacy. On the other hand, it may have a significant impact. (For example in using Public Key Infrastructure, Smart Cards, and electronic signatures, new personal information is collected on the individual which will need appropriate safeguards). Contact your office's Privacy Act Officer for clarification.

Narrative Statement Information: This information is used when submitting a narrative statement (see 383 DM 5, Appendix 2, A.3). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative.

**6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

Most systems provide the capability to identify, locate, and monitor individuals (e.g., audit trail systems/applications). Generally, the Core Terminal Table that is embedded in a system contains the Security Information Record [SIR] that identifies and authenticates the users to the system. Check your security procedures for information to respond to this question.

Narrative Statement Information: This information is used when submitting a narrative statement to OMB and Congress for new and major amendments to Privacy Act systems of records (see 383 DM 5, Appendix 2, A.3). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative.

**7) What kinds of information are collected as a function of the monitoring of individuals?**

The DOI IT Security Plan describes the audit trail process. In response to this question provide what audit trails are maintained to record system activity and user activity including invalid logon attempts and access to data. The IT Security C&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

**8) What controls will be used to prevent unauthorized monitoring?**

Rules of Behavior are required as part of the IT Security C&A process. Responsibility is placed on managers of systems to ensure no unauthorized monitoring is occurring.

Narrative Statement Information: This information is used when submitting a narrative statement (see 383 DM 5, Appendix 2, A.5). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative

**9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

If you do not know the Privacy Act systems of records (SOR) notice, contact your office's Privacy Act Officer. The Privacy Act requires publication of a notice in the *Federal Register* describing each SOR subject to the Act (see 383 DM 5). Any officer or employee who knowingly and willfully maintains a SOR without meeting the Privacy Act notice requirements (5 U.S.C. 552a(e)(4)) is guilty of a misdemeanor and may be fined up to \$5,000. Also refer to information for question D. 8 above.

If a name or other personal identifier is not used to retrieve information, it is possible that the system is not a Privacy Act system. However, even though information may not fall under the Privacy Act's protection and requirements, certain information may be protected from disclosure under the Freedom of Information Act.

**10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

The system may already have a Privacy Act system of records notice that applies to it. However, the Privacy Act requires that amendments to an existing system must also be addressed in a *Federal Register* notice (see the DOI Privacy Act Manual Section 383 DM 5.3). Consult with your bureau/office Privacy Act Officer.

## **F. ACCESS TO DATA:**

- 1) Who will have access to the data in the system?** (E.g., contractors, users, managers, system administrators, developers, tribes, other)

Also consider “other” users who may not be as obvious as those listed above, such as the GAO or the Inspector General. “Other” may include database administrators or IT System Security Managers. Also include those listed in the Privacy Act system of records notice under the “Routine Use” section when a Privacy Act system of records notice is required. The more comprehensive the list, the better it is.

- 2) How is access to the data by a user determined?** Are criteria, procedures, controls, and responsibilities regarding access documented?

For the most part, access to data by a user within the DOI is determined by the “need-to-know” requirements of the Privacy Act, the user’s profile based on the user’s job requirements and managerial decisions. The criteria, procedures, controls and responsibilities regarding access must be documented to comply with the intent of the Computer Security Act of 1987 [Public Law 100-235] for standards and guidelines on security and privacy. What criteria will the manager and system security person use to decide on access to the data, for example?

The Departmental IT Security Manual at 375 DM 19 indicates that the system manager is responsible for ensuring that access to information and data is restricted to authorized personnel on a “need-to-know” basis.

Narrative Statement Information: This information is used when submitting a narrative statement (see 383 DM 5, Appendix 2, A.5.). If the system already has a Privacy Act system of records notice, then the response to this question should reflect the information already in the narrative.

- 3) Will users have access to all data on the system or will the user’s access be restricted? Explain.**

Usually, a user is only given access to certain data on a “need-to-know” basis either in a system/application/process; and therefore, it is considered to be restricted. System administrators may be afforded access to all of the data depending upon the system and/or application. However, system administrators and other users may not need to have access to all the data. For more guidelines on this, refer to the Federal Information Processing Standards [FIPS] Publications at <http://www.itl.nist.gov/fipspubs/0-toc.htm>.

The IT Security Plan describes the practice of applying logical access controls. Logical access controls are system-based means by which the ability is explicitly enabled or restricted.

**4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)**

According to OMB Circulars A-123 and A-130, every system/application/process that uses data must have some sort of control to prevent the misuse of the data by those having access to the data. For instance, in computerized systems the Security Information Record (SIR) is part of the Core Storage Terminal Table. The SIR is the automated tool that identifies and authenticates an individual for the system and is transparent to the user. Describe these in response to this question.

The IT Security Plan describes the practice of audit trails. Audit trails maintain a record of system activity and user activity including invalid logon attempts and access to data. The C&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

Are there privacy and security awareness controls such as training materials for personnel? All employees, including contractors, have requirements for protecting Privacy Act protected information (see DOI Privacy Act regulations at 43 CFR 2.52: Conduct of Employees, and 43 CFR 2.53: Government Contracts). Describe the controls in place. This will be helpful in completing Exhibit 300, Part II. C. 2. (D).

**5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system?**

If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

When a contract provides for the operation of a SOR on behalf of the DOI, the Privacy Act requirements and Departmental regulations on the Privacy Act must be applied to such a system (see DOI Privacy Act regulations at: 43 C.F.R.2.53: Government Contracts). The Federal Acquisition Regulations (FAR) also require that certain information be included in contract language and certain processes must be in place (see FAR 48 C.F.R.24.102(a) and DOI Acquisition Regulation at 48 C.F.R.1424.1).

This will be helpful in completing Exhibit 300, Part I. F. 2. and Part II. C. 2. (D).

**6) Do other systems share data or have access to the data in the system? If yes, explain.**

This question deals primarily with interfaces between processes, systems, and applications. If it is unknown to you whether or not systems share data, you can either contact the business owner of the data, or you can contact the IT specialist who knows what other interface goes on between the systems/applications. As an example, if your system/application shares data with another system/application, ask yourself whether you have access to the data in the interfaced system/application. If so, then your answer is

yes and an explanation is needed. You may also need to have a copy of any Memorandum of Understanding or sharing agreement that may be in force/effect, if other agencies are interfacing with this system.

For further information on interfaces and applicable guidance, refer to FIPS Publication 191, Local Area Networks. The publication contains definitions and explanations that may assist you (see FIPS publications at <http://www.itl.nist.gov/fipspubs/0-toc.htm>).

You must first review appropriate Privacy Act SOR notices to determine whether any information that may come from an existing Privacy Act SOR allows that information to be exchanged and used for these new purposes or uses. There are statutory restrictions on use and disclosure of information that comes from a Privacy Act SOR. Please consult with your appropriate bureau/office Privacy Act Officer. (Refer to Privacy Act disclosure restrictions at 43 CFR 2.56 and 383 DM 7).

This will be helpful in completing Exhibit 300, Part II. B. 5.

**7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

Although all employees who have access to information in a Privacy Act system have some responsibility for protecting personal information covered by the Privacy Act (see 43 CFR.2.52: Conduct of Employees), often the information owner and system manager (identified in the Privacy Act system of records notice) share responsibilities.

For system manager responsibilities identified by the Privacy Act refer to DOI Privacy Act Manual Sections 383 DM 1.4.F., 3.6, and 4.4.C. and DOI Privacy Act regulations at 43 CFR 2.48, 2.51, 2.52, 2.56 and 2.57 - 2.77. The DOI Information Resource Manual Section 376 DM 13: Automated Information Systems Management Accountability identifies the IT related responsibilities of a system manager and system owner.

**8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?**

This question deals primarily with agencies outside of the DOI and will include the oversight agencies. If you are not sure if other agencies share the data or have access to the data in this system/application/process, you should contact either the data owners or the IT services group.

You must first review appropriate Privacy Act SOR notices to determine whether any information that may come from an existing Privacy Act SOR allows for its exchange and use for these new purposes or uses. There are statutory restrictions on use and disclosure of information that come from a Privacy Act SOR. Please consult with your appropriate bureau/office Privacy Act Officer. (Refer to Privacy Act disclosure restrictions at 43 CFR 2.56 and 383 DM 7).

**9) How will the data be used by the other agency?**

Has DOI entered into a Matching Agreement by sharing this data with another agency? For Departmental guidelines on Computer Matching programs refer to DOI Privacy Act Manual Section 383 DM Ch.12. Also refer to OMB Memo of December 20, 2000: M 01-05 on “Interagency Sharing of Personal Data” at <http://www.whitehouse.gov/OMB/memoranda/m01-05.html>; and DOI IRM Bulletin No. 2001-002 at <http://www.doi.gov/ocio/bulletins/2001-002bul.htm>.

**10) Who is responsible for assuring proper use of the data?**

This may be stipulated in the language contained in the agreement (e.g. Head of the Bureau, or Program Manager). Refer to OMB Circulars A-123: Management Accountability, and A-130: Management of Federal Information Resources.

## SECTION III

### Web Links to Privacy Policy Resources

#### **BUDGET PROCESS AND PRIVACY REQUIREMENTS**

- 1) See required privacy plans at Office of Management and Budget (OMB) Circular A-11, Preparation and Submission of Budget Estimates, July 2000 (see sections 31.8, 50.1, 50.2 & 58.3 and 300.1 at <http://www.whitehouse.gov/omb/circulars/a11/02toc.html>)

#### **CHILDREN'S ONLINE PRIVACY PROTECTION ACT**

- 2) Federal Trade Commission guidance on complying with the Children's On-Line Privacy Protection Act: <http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm>
- 3) Department of the Interior (DOI) IRM Bulletin No. 2000-004, Interim Guidance on Children's Privacy Statements on Websites, June 5, 2000: <http://www.doi.gov/ocio/bulletins/2000-004bul.htm>

#### **DEPARTMENT OF THE INTERIOR GUIDELINES**

- 4) The DOI regulations for implementing the Privacy Act can be found at 43 CFR Part 2, Subpart D: <http://www.doi.gov/foia/43cfrsub.html>.
- 5) The DOI manual sections on the Privacy Act can be found at 383 DM Ch. 1-13. Copies can be obtained from your Privacy Act Officer or Directives Liaison. It is also posted on the DOI Privacy Program Homepage at <http://www.doi.gov/ocio/privacy/manual/index.html>
- 6) The DOI Privacy Program Homepage: <http://www.doi.gov/ocio/privacy/index.html>
- 7) DOI Information Technology Security Homepage: <http://www.doi.gov/ocio/security/>
- 8) DOI Webmasters Council Homepage: <http://www.doi.gov/ocio/index.html>
- 9) DOI Privacy Act system of records notices: [http://www.access.gpo.gov/su\\_docs/aces/PrivacyAct.shtml](http://www.access.gpo.gov/su_docs/aces/PrivacyAct.shtml)
- 10) DOI Freedom of Information Act Homepage: <http://www.doi.gov/foia/>
- 11) DOI Office of the Chief Information Officer bulletins: <http://www.doi.gov/ocio/bulletins/index.html>
- 12) DOI IRM Bulletin on Processing FOIA Requests for Personal and Personnel-Related Information, March 1, 1996: IRM Bulletin No. 1996-004: <http://www.doi.gov/ocio/bulletins/9604.htm>
- 13) DOI IRM Bulletin No. 2001-004, Protecting Sensitive Data When Transferring, Donating, or Disposing of Computer Equipment, June 12, 2001: <http://www.doi.gov/ocio/bulletins/2001-004bul.htm>

## **FEDERAL CONTRACTS AND THE PRIVACY ACT**

- 14) The Privacy Act, Section (m) addresses accountability for Privacy Act systems of records maintained by persons other than agency personnel:  
<http://www4.law.cornell.edu/uscode/5/552a.html>
- 15) The Federal Acquisition Regulations (FAR) requires that when an agency contracts for the design, development, or operation of a system of records on individuals on behalf of the agency to accomplish an agency function, the agency must apply the requirements of the Privacy Act to the contractor and its employees working on the contract (FAR 48 CFR 24.102(a)): <http://www.arnet.gov/far/loadmainre.html>
- 16) FAR Contracting Officer and System Manager responsibilities (FAR at 48 CFR 24.103): <http://www.arnet.gov/far/loadmainre.html>
- 17) DOI Privacy Act regulations on contracts (43 CFR 2.53):  
<http://www.doi.gov/foia/43cfsub.html>
- 18) DOI Acquisition Regulations (DIAR) 1452.224-1:  
<http://www.ios.doi.gov/pam/1452-3.html>

## **GEOGRAPHIC INFORMATION SYSTEMS AND PRIVACY POLICY**

- 19) Office of Management and Budget Circular A-16 dated August 19, 2002 on “Coordination of Geographic Information and Related Spatial Data Activities”. Refer to Sections 2.a. and 8.a.7 of the Circular.
- 20) Federal Geographic Data Committee Privacy Policy established in 1999 at  
<http://www.fgdc.gov/fgdc/policies/privacypolicy.pdf>
- 21) Urban Regional Information Systems Association “Code of Ethics” (see section IV on Privacy) at [http://www.urisa.org/ethics/code\\_of\\_ethics.htm](http://www.urisa.org/ethics/code_of_ethics.htm)

## **GOVERNMENT GUIDELINES**

- 22) The Privacy Act of 1974, as amended (5 U.S.C. 552a):  
<http://www4.law.cornell.edu/uscode/5/552a.html>
- 23) OMB Privacy Page: <http://www.whitehouse.gov/omb/privacy/index.html>
- 24) OMB Circular A-130. See Appendix I for implementing the Privacy Act and transmittal memorandum:
  - <http://www.whitehouse.gov/OMB/circulars/a130/a130trans4.html> (Transmittal)
  - [http://www.whitehouse.gov/omb/circulars/a130/a130appendix\\_i.html](http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.html) (Privacy)
  - [http://www.whitehouse.gov/omb/circulars/a130/a130appendix\\_ii.html](http://www.whitehouse.gov/omb/circulars/a130/a130appendix_ii.html) (GPEA)
  - [http://www.whitehouse.gov/omb/circulars/a130/a130appendix\\_iii.html](http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html) (Security)

- 25) OMB Privacy Act regulations on personnel records (5 CFR 297):  
<http://www.opm.gov/feddata/cfr297.txt>
- 26) Government Privacy Act system notices online:  
[http://www.access.gpo.gov/su\\_docs/aces/aces140.html](http://www.access.gpo.gov/su_docs/aces/aces140.html)
- 27) Selective recent privacy initiatives by the U.S. Government:  
[http://www.cio.gov/documents/selective\\_privacy\\_init\\_sept\\_2000.html](http://www.cio.gov/documents/selective_privacy_init_sept_2000.html)
- 28) Federal CIO Council Subcommittee on Security, Privacy, and Critical Infrastructure: [http://www.cio.gov/documents/committee\\_spci.html](http://www.cio.gov/documents/committee_spci.html)
- 29) OMB documents on information policy and technology:  
<http://www.whitehouse.gov/OMB/inforeg/index.html>
- 30) Federal Trade Commission privacy initiatives:  
<http://www.ftc.gov/privacy/index.html>
- 31) General Services Administration's listing of IT policy documents (laws, Executive Orders, OMB memos, etc.): <http://www.itpolicy.gsa.gov/itpolicy.htm>
- 32) Government Printing Office Drafting Handbook (see Ch. 3 on guidelines for Privacy Act System of Records Notices):  
<http://www.nara.gov/fedreg/ddhhome.html>

#### **INTERAGENCY DATA SHARING**

- 33) OMB memo on Interagency Sharing of Personal Data, December 20, 2000:  
<http://www.whitehouse.gov/omb/memoranda/m01-05.html>
- 34) DOI IRM Bulletin No. 2001-002, Guidance on Inter-Agency Sharing of Personal Data, and Privacy Protection Measures in System Development and Applications, February 26, 2001: <http://www.doi.gov/ocio/bulletins/2001-002bul.htm>
- 35) General Accounting Office (GAO) Report of April 2001 (GAO-01-12SP) on Data Linkage and Privacy: <http://www.gao.gov/new.items/d01126sp.pdf>.

#### **INTERNET AND PRIVACY**

- 36) Letter from OMB Office of Regulatory Affairs Administrator, John Spotila, on the use of "cookies" on Federal Government web sites, September 5, 2000:  
[http://www.whitehouse.gov/omb/inforeg/cookies\\_letter90500.html](http://www.whitehouse.gov/omb/inforeg/cookies_letter90500.html)
- 37) DOI IRM Bulletin No. 2001-001, Policy Use of "Persistent Cookies" on Interior Web Sites, March 1, 2001: <http://www.doi.gov/ocio/bulletins/2001-001bul.htm>
- 38) OMB memo on Privacy Policy and Data Collection on Federal Web Sites, M-00-13, June 22, 2000: at <http://www.whitehouse.gov/omb/memoranda/m00-13.html>

- 39) OMB memo on Privacy Policies on Federal Web Sites, M-99-18, June 2, 1999: <http://www.whitehouse.gov/omb/memoranda/m99-18.html>
- 40) OMB memo on Privacy and Personal Information in Federal Records, M-99-05, May 14, 1998: <http://www.whitehouse.gov/omb/memoranda/m99-05.html>
- 41) GAO Report on Internet Privacy, Agency Efforts to Implement OMB's Privacy Policy: <http://www.gao.gov/nes.items/d01113t.pdf>
- 42) List of GAO reports on E-Government: <http://www.gao.gov/index.htm>
- 43) Congressional Internet Caucus Advisory Committee Briefing Book on E-Government Issues dated March 22, 2001 (see section on Privacy): <http://www.netcaucus.org/books/egov2001/>
- 44) The official Departmental web privacy policy statement: <http://www.doi.gov/footer/privacy.html>
- 45) The official Departmental web disclaimer statement: <http://www.doi.gov/footer/disclaim.html>
- 46) DOI IRM Bulletin No. 2001-005, System Warning Banner, June 12, 2001: <http://www.doi.gov/ocio/bulletins/2001-005.pdf>

#### **PRIVACY PLANNING AND ASSESSMENTS**

- 47) OMB Circular A-130, Management of Federal Information Resources, (revised) November 28, 2000: <http://www.whitehouse.gov/OMB/circulars/a130/a130trans4.html>
- 48) Federal Chief Information Officer Council Model Information Technology Privacy Impact Assessment (PIA) (see Section. V. Checklist) at [http://www.cio.gov/Documents/pia\\_for\\_it\\_irs\\_model.pdf](http://www.cio.gov/Documents/pia_for_it_irs_model.pdf).
- 49) DOI Office of the CIO Bulletin 2001-002: Interagency Sharing of Personal Information and Privacy Impact Assessments, February 26, 2001: <http://www.doi.gov/ocio/bulletins/2001-002bul.htm>
- 50) Department of Justice Guide on "Legal Considerations in Designing and Implementing Electronic Processes (implementation of GPEA) (see C. Assessing the Significance of Risk, and II. Legal Issues to Consider in "Going Paperless" at <http://www.cybercrime.gov/eprocess.htm>
- 51) DOI Office of the CIO paper on the Privacy Challenge for E-Government: <http://www.netcaucus.org/books/egov2001/pdf/key.pdf>