



Privacy Impact Assessment

Version Number: [x.x]

Version Date:

Issued by:

[Senior Official for Privacy (if designated, otherwise the privacy point of contact)]

Introduction

The Department of the Interior requires a Privacy Impact Assessment (PIA) to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle.

Need more guidance? The [DOI PIA Guide](#) provides more in-depth information on when and why PIAs are required, legal references and guidelines for filling out this template. You can also email the [Departmental Privacy Office](#) for more help.

I. Determine if a PIA is required

Does this system collect or maintain information from any of the following?

- Members of the general public
- Federal personnel and/or Federal contractors
- Volunteers

No Complete *only* Section 1 and Section 6.

Yes Please complete *all* sections:

| | |
|--|----|
| Section 1. Contact Information | 4 |
| Section 2. General System Information | 5 |
| Section 3. Summary of System Data | 8 |
| Section 4. Maintenance and Administrative Controls | 13 |
| Section 5. PII Safeguards and Liabilities..... | 15 |
| Section 6. Approval | 20 |

Section 1. Contact Information

System Name

Date

Organization

Enter the contact information for the primary person responsible for answering questions about PII in this system.

First Name

Last Name

Title

Email Address

Phone

Address

City

State/Territory

Zip

Section 2. General System Information

2.1 Is this a new PIA or a modification of an existing PIA?

New

Modification Name of existing PIA:

2.2 What is this system for?

2.3 Legal Authorities

Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

| Authority | Citation/Reference |
|--|--------------------|
| Statute | |
| Executive Order | |
| Federal Regulation | |
| Memorandum of Understanding/agreement | |
| Other (summarize and provide copy of relevant portion) | |

2.4 Other system information

(a) System registered in CSAM?

Yes

No

(b) Published Privacy Act System of Records Notice (SORN) required?

Yes

No

If Yes, list Privacy Act SORN Identifier(s):

(c) OMB Control Number required?

Yes

No

If yes, enter OMB control number:

2.5 Enter the UII Code and the System Security Plan (SSP) Name

The completed PIA, associated system of records notice(s), and any other supporting artifacts must be entered into the CSAM system for each registered system or application.

UII Code

Systems Security Plan (SSP) name

2.7 List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Enter "None" if no subsystems or applications are hosted. For General Support Systems (GSS) be sure to include all hosted major applications, minor applications, or other subsystems, and describe the purposes and types of PII if any. Privacy risks must be identified and adequately addressed for each hosted application or subsystem identified in the GSS PIA. It is strongly recommended that a separate PIA be conducted specifically for each hosted application or subsystem that contains significant amounts of PII. In any case, the GSS PIA must identify all hosted applications, describe the relationship, and reference or append the PIAs conducted for the hosted applications. The GSS PIA and associated PIAs must be reviewed and approved by all officials as appropriate; and all related PIAs, SORNs and supporting artifacts must be entered into CSAM.

| SUBSYSTEM NAME | PURPOSE | CONTAINS PII? | IF YES, DESCRIBE |
|----------------|---------|---------------|------------------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Section 3. Summary of System Data

3.1 Indicate below what PII is collected, maintained, or disseminated.

(Check all that apply.)

| | | |
|------------------------|---------|--------------|
| Name | Address | Phone number |
| Email address | Gender | Age |
| Social Security Number | | |
| Other (describe) | | |

3.2 Indicate the sources for the PII. (Check all that apply)

(a) Directly from the individual about whom the information pertains:

| | | |
|------------------|--------|---------------------|
| In person | Phone | Hard copy: mail/fax |
| Email | Online | |
| Other (describe) | | |

(b) Government sources:

Within the bureau

Within another federal entity or entities

Within the agency

State, local, tribal

Foreign

Other (describe)

(c) Non-government sources:

Members of the public

Commercial data brokers

Public media, interest

Private sector

Other (describe)

3.3 How will the PII be collected?

3.4 With whom will the PII be shared, both within DOI and outside DOI?

| Recipient | Case-by-case | Bulk transfer | Direct access | Other (specify) |
|--------------------------------------|--------------|---------------|---------------|-----------------|
| DOI | | | | |
| Other Federal agencies | | | | |
| State or local tribal govt. entities | | | | |
| Other Federal agencies | | | | |
| Public | | | | |
| Private sector | | | | |
| | | | | |
| | | | | |

3.5 Do individuals have an opportunity to consent to providing PII?

Yes: Specify how

No: Specify why not

3.6 Can individuals “opt-out” by declining to provide PII or by consenting only to a particular use?

Yes: Specify how

No: Specify why not

3.7 What information is provided to an individual when asked to provide PII data?

3.8 PII mapping

| Component | Does this function collect or store PII? | | | |
|-----------|--|------------------------------|------------|--|
| | Type of PII | Reason for Collection of PII | Safeguards | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Section 4. Maintenance and Administrative Controls

4.1 Are data collected from sources other than DOI records verified for accuracy?

Yes Specify how

No Specify why not

4.2 Are data collected verified for accuracy?

Yes Specify how

No Specify why not

4.3 Is the PII current? How is this determined?

4.4 What are the retention periods of PII for this system? Under what guidelines are the retention periods determined? Who establishes the retention guidelines?

4.5 What are the procedures for disposition of the PII at the end of the retention period? How long will any reports that contain PII be maintained? How is the information disposed (e.g., shredding, degaussing, overwriting, etc.)? Who establishes the decommissioning procedures?

4.6 Briefly describe privacy risks and information handling practices at each stage of the “information lifecycle” (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

Section 5. PII Safeguards and Liabilities

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

Yes Specify how

No Specify why not

5.2 Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

Yes Specify how

No Specify why not

5.3 Will the new data be placed in the individual's record?

Yes Specify how

No Specify why not

5.4 Can the system make determinations about individuals that would not be possible without the new data?

Yes Specify how

No Specify why not

5.5 How will the new data be verified for relevance and accuracy?

5.6 Are the data or the processes being consolidated?

Yes Specify how

No Specify why not

5.7 Who will have access to data in the system or electronic collection?

5.8 How is user access to data determined? Will users have access to all data or will access be restricted?

5.9 Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

Yes Specify how

No Specify why not

5.10 Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

Yes Specify how

No Specify why not

5.11 Will this system provide the capability to identify, locate and monitor individuals?

Yes Specify how

No Specify why not

5.12 What kinds of information are collected as a function of the monitoring of individuals?

5.13 What controls are in place to prevent the misuse (e.g., browsing) of data by those having access?

5.14 How will the PII be secured?

- 5.15 Who will be responsible for protecting the privacy rights of the individuals whose PII is collected, maintained, or shared on the system? Have policies and/or procedures been established for this responsibility and accountability? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.
- 5.16 Who is responsible for assuring safeguards for the PII? Who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

Section 6. Approval

6.1 Information System Owner

First Name

Middle Name

Last Name

Title

Email

Bureau / Agency

Phone

Signature

Date

6.2 Information System Security Officer

First Name

Middle Name

Last Name

Title

Email

Bureau / Agency

Phone

Signature

Date

6.3 Privacy Officer

First Name

Middle Name

Last Name

Title

Email

Bureau / Agency

Phone

Signature

Date

6.4 Reviewing Official

First Name

Middle Name

Last Name

Title

Email

Bureau / Agency

Phone

Signature

Date