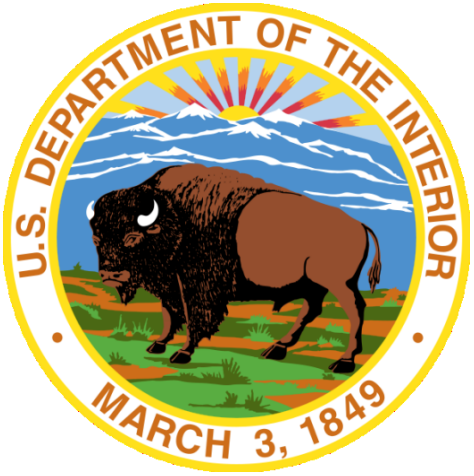
DEPARTMENT OF THE INTERIOR

Privacy Impact Assessment Guide



Departmental Privacy Office
Office of the Chief Information Officer

September 30, 2014

Table of Contents

INTRODUCTION

Federal government agencies are required under Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Chapter 36) to conduct a Privacy Impact Assessment (PIA) before developing or procuring information technology (IT), or initiating new information collections that use IT, that collects, maintains or disseminates personally identifiable information (PII). A completed PIA demonstrates that the agency has evaluated privacy risks and incorporated protections commensurate with those risks to ensure sufficient safeguards are in place for the protection of personal information as agencies implement citizen-centered electronic Government. A PIA also ensures government transparency by informing the public of the information collected about them, and any impact agency systems or information collections may have on their personal privacy. PIAs confirm that information collected is protected and used for the purpose intended, that the information remains timely, relevant, accurate and complete, and that agencies maintain it only as long as it is needed.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, requires Federal agencies to implement privacy controls for information systems to protect the PII of individuals collected and maintained by organizations in accordance with Federal privacy laws, regulations, policies and guidelines. Organizations may tailor the privacy controls to meet their defined and specific needs at their organization level, and implementation of privacy controls may vary based on legal authorities and distinct mission/business or operational needs. Identifying and documenting privacy controls during the PIA process will ensure appropriate privacy protections are in place to protect PII during the information life cycle, and demonstrate compliance with Federal privacy requirements and standards.

The Departmental Privacy Office partners with Bureau/Office privacy staff to assess all new or proposed programs, systems or applications for privacy risks, and recommends methods for handling PII to protect individual privacy and mitigate risks to privacy information. PIAs are completed and maintained by the Bureau/Office Privacy Office where the information system is located. A copy of the completed PIA, and any associated system of records notice (SORN), must be entered into the Cyber Security Assessment and Management (CSAM) system for every information system registered.

This revised Department of the Interior (DOI) PIA Guide provides detailed guidance and reflects updates on new policy and best practices for conducting privacy impact assessments to ensure DOI compliance with the E-Government Act of 2002, the Privacy Act of 1974 (5 U.S.C. 552a), Office of Management and Budget (OMB) mandates, NIST SP 800-53 Revision 4, and other applicable privacy laws, regulations, and standards. This Guide supersedes any previously issued guidance and must be followed for all new and updated PIAs conducted at DOI.

Section 1.0 - What is a Privacy Impact Assessment (PIA)

The PIA is an analysis of how information is handled, or specifically it is an assessment of how PII is collected, used, maintained and disseminated. The PIA is an important tool used to identify, evaluate and analyze potential privacy risks associated with the development or use of information systems or applications. The objective of the PIA is to assist DOI Information System Owners and program managers to identify and address information privacy when planning, developing, implementing, and operating agency information management systems that maintain information on individuals, and consider privacy implications throughout the development life cycle of a system in order to mitigate any impact on individual privacy. The PIA also facilitates government transparency as it informs the public on what information DOI is collecting or maintaining, why the information is collected, how the information is used, how the information is accessed and stored, and how the information is safeguarded.

The PIA process helps to identify sensitive systems to ensure that appropriate information assurance measures are in place, such as encrypted storage media, secured transmission, special handling instructions, and access controls.

In addition to a completed PIA, the security plan or business rules should include specific access controls and disclosure restrictions for protection of privacy information and implementing Privacy Act requirements when applicable. Identifying sensitive information and awareness of the proper ways of handling that sensitive information are major steps in ensuring that information is protected.

The goals accomplished in completing a PIA include:

- Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk and of options available for mitigating that risk;
- Accountability for privacy issues;
- Analyzing both technical and legal compliance with applicable privacy laws and regulations, as well as accepted privacy policy; and
- Providing documentation on the flow of personal information and information requirements within DOI systems.

The PIA process requires collaboration between the Information System Owner, Program Manager, Information System Security Officer, the Bureau/Office Records Officer, the Bureau/Office Privacy Officer, and the Departmental Privacy Office to ensure potential privacy risks are addressed and appropriate privacy protections are implemented. PIAs must be updated when changes are made to systems that may raise new privacy risks, when there is a change in

information handling practices or information collection or at a minimum at least every three years.

1.1 Personally Identifiable Information

Personally identifiable information (PII) is information in a program, system, collection, or technology that permits the identity of an individual to be directly or indirectly inferred, including any other information which is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or employee or contractor to the Department.

Any information or collection of information that connects to an individual is PII. Examples of PII include but are not limited to: name, alias, username, home mailing address, personal telephone number, personal email address, social security number (SSN), date of birth, place of birth, nationality, passport number, tribal enrollment number, bank account number, credit card number, vehicle license number, internet protocol addresses, biometric identifiers (fingerprints), photographic facial images, work or educational history, and any information that may be linked with other information to identify an individual.

PII may be much broader than "private" information, which is information that an individual would prefer not to be known to the public due to its personal or intimate nature. PII identifies a person or can be used in conjunction with other information to identify a person, regardless of whether a person would want it disclosed. For example, a license plate number is personally identifiable information because it indirectly identifies an individual, but it is not deemed "private" because it is visible to the public. PIAs require an analysis of privacy risks associated with agency collection and use of privacy protected information or PII, whether or not it is "private information" considered sensitive by individuals.

1.2 PIAs and the Privacy Act

The Privacy Act of 1974 requires agencies to publish Systems of Records Notices (SORNs) in the *Federal Register* that describe the categories of records on individuals that they collect, use, maintain, and disseminate. Generally, the requirements to conduct a PIA are broader than the requirements for SORNs. The PIA requirement is triggered by the collection or maintenance of information within an electronic system, while the SORN requirement is triggered by the collection or maintenance of information on individuals that is actually *retrieved* from any paper or electronic system by a personal identifier. Any time a change or update to information technology raises new privacy risks, an updated PIA must be completed to analyze these new risks - even if the collection of information remains the same. The SORN covering the system must also be reviewed and updated if necessary to ensure completeness and accuracy.

Section 2.0 - When to Conduct a PIA

A PIA must be conducted for all DOI systems, including law enforcement or other sensitive systems, to ensure privacy implications are considered and appropriately addressed. Section 208 of the E-Government Act and OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", require agencies to conduct a PIA when:

- Developing or procuring any new technologies or systems that handle or collect PII. Conducting a PIA at the beginning of the development process allows the Privacy Office, program management, and system developers to ensure that the information is handled appropriately. The PIA should show that privacy was considered from the beginning stage of system development. The PIA also provides for a framework to conduct ongoing reviews of systems or programs.
- Reviewing Information Collection Requests (ICRs) that gather PII including forms under the Paperwork Reduction Act (PRA). If the form or ICR is not covered by an existing PIA and SORN, a new PIA will be required.
- Developing system changes that affect PII or create privacy risk. For example, if a program or system adds additional sharing of information either with another agency or incorporates commercial data from an outside data aggregator, or if an organization decides to collect new information or update its existing collections as part of a rulemaking. The PIA should discuss how the management of these new collections ensures conformity with privacy law. Other examples include converting paper–based records to electronic systems; functions that change anonymous information into PII; altered business processes that result in databases holding PII that are merged, centralized, or matched with other databases; user-authenticating technology (password, digital certificate, biometric) newly applied to an electronic information system; or new PII added to a collection that raises the risks to personal privacy.

It is important to note that even if it is not apparent that a system collects or maintains PII, there could be instances where an interface, new source, aggregation, or evolving use may raise privacy risks that must be evaluated through a PIA. Examples of technology systems that generally have privacy implications are human resources, payroll, and law enforcement systems, or systems that perform data mining, data aggregation or geospatial tracking.

Note that PIAs must address and document privacy controls implemented for information systems, and the privacy controls must be approved by the Senior Agency Official for Privacy (SAOP) as a precondition to granting an Authority to Operate (ATO).

2.1 Systems That Do Not Contain PII

Some information systems do not contain information that is identifiable to individuals and will not require a full PIA. To ensure that a thorough review is made of all IT systems for PII on individuals, the Information System Owner should complete the first section of the PIA form and submit it to the Bureau/Office Privacy Officer for review to determine further privacy compliance documentation. This properly documents that an Information System Owner assessed whether the system contains PII and requires a full PIA. This preliminary assessment is also incorporated into the DOI IT Security Assessment and Authorization (A&A) process, which is the process by which the Department assures its information technology systems meet appropriate security and operating standards. This verifies that a review for any information on individuals was already completed for the system.

Section 3.0 - Documents Associated with a PIA

3.1 System of Records Notice

The Privacy Act of 1974 requires Federal agencies to publish a SORN in the *Federal Register* for systems of records denoting the categories of records on individuals that they collect, use, maintain or disseminate the safeguards to protect the information, the location of the system, the system manager, and how individuals can obtain notice and access to records about themselves.

Some systems may maintain PII on individuals but are not subject to the provisions of the Privacy Act. The requirements of the Privacy Act are triggered by the retrieval of information by use of a name or other identifier assigned to an individual. Any system that maintains information about individuals that is subject to the Privacy Act must have a published SORN, and must collect, use, maintain and disseminate information in accordance with that SORN. When conducting a PIA on a new or updated system, the associated SORN must be reviewed to ensure the system handles information in accordance with the SORN, or to determine whether the SORN should be revised to reflect the changes to the system.

3.2 OMB Budget Submissions – Exhibit 300s

Although PIAs will be completed for all information systems, the OMB only requires that Exhibit 300 budget submissions include PIAs for projects that collect and manage information on individual members of the public that is identifiable to the individual.

For projects that collect and manage information on individual members of the public, OMB requires that a PIA be submitted with Exhibit 300s for budget requests (see OMB Circular A-11, "Preparing, Submitting, and Executing the Budget", at http://www.whitehouse.gov/omb/circulars_a11_current_year_a11_toc).

3.3 Paperwork Reduction Act Submissions

If you are collecting information from members of the public, contact your Bureau/Office Information Collection Clearance Officer to ensure that you have 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 1995 establishes requirements for collecting the same information from ten (10) or more persons – this does not include Federal employees acting in their official capacity.

The E-Government Act also requires agencies to conduct a PIA on any new collection of information from ten (10) or more members of the public using information technology. This requirement does not include collections of information from agencies, organizations, or employees of the Federal government. See OMB M-03-22 for more information on the E-Government Act and Paperwork Reduction Act interface.

3.4 DOI IT Security Assessment and Authorization Process

The DOI IT Security A&A process is an integral part of DOI's information security program. It is an important activity that supports the risk management process for a detailed security review of information systems and a comprehensive assessment of the management, operational and technical security and privacy controls. The A&A process requires a completed PIA to ensure effective controls are in place to protect privacy and that systems are compliant with requirements of the E-Government Act, the Privacy Act, OMB mandates, NIST standards, and DOI privacy and security policies. The PIA will demonstrate compliance with privacy requirements and the implementation of appropriate privacy controls for DOI information systems.

Section 4.0 - Roles and Responsibilities

Since the requirements of a PIA must be addressed during the early stages of system development, ideally the Information System Owner and system developer will complete the assessment. Information 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 requirements presents any threats to privacy. Information System Owners and system developers will need to coordinate certain responses with the Bureau/Office Privacy Officer, Information Collection Clearance Officer, Information System Security Officer or Chief Information Security Officer, Records Officer, and possibly the Chief Information Officer.

4.1 Information System Owner

The Information System Owner is the official responsible for the overall procurement, development, integration, modification, or operation and maintenance of information systems. The Information System Owner is responsible for completing the PIA and implementing the legal information resources management requirements such as Privacy, Security, Records Management, Freedom of Information Act, and data administration. To ensure complete and accurate PIAs are conducted, Information System Owners must work closely with Bureau/Office Privacy Officers, Information System Security Officers or Chief Information Security Officers, Information Collection Clearance Officers and Records Officers. The Information System Owner must work with these officials to resolve any identified privacy or security risks. The Information System Owner must also ensure that all appropriate reviews and surnames are obtained.

Information System Owner responsibilities include, but are not limited to:

- Collaborating with the Bureau/Office Privacy Officer to ensure privacy risks are properly assessed and identifying applicable Privacy Act SORNs for systems subject to the provisions of the Privacy Act.
- Collaborating with the Privacy Act System Manager to ensure Privacy Act records are maintained in accordance with the provisions of the Privacy Act and the published SORN.
- Collaborating with the Information System Security Officer and Bureau/Office Chief Information Security Officer to ensure appropriate security and privacy controls are implemented to restrict access, properly manage and safeguard PII maintained within the system, document privacy controls in PIAs for SAOP approval, and provide a completed PIA for the DOI IT Security A&A process.
- Identifying records disposition schedules with their Bureau/Office Records Officer.
- Consulting with the Bureau/Office Information Collection Clearance Officer for information collection approvals by OMB if necessary (usually a 180 day process).
- Reporting any suspected or confirmed compromise of privacy data to DOI-CIRC within one hour of discovery in accordance with OMB M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments”, OMB M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”, and the DOI Privacy Loss Mitigation Strategy.

4.2 Privacy Act System Manager

The Privacy Act System Manager is the official with administrative responsibility for managing and protecting Privacy Act records, whether in electronic or paper format, and for meeting the requirements of the Privacy Act and the published SORN. The Privacy Act System Manager is usually identified in the published SORN; however, this responsibility may be further delegated to personnel within an agency, program or office. For Privacy Act System Manager responsibilities, refer to the Departmental Manual Privacy Act Sections, 383 DM Chapters 1-13, and DOI Privacy Act regulations at 43 CFR Part 2.

Privacy Act System Manager responsibilities include, but are not limited to:

- Safeguarding the records they are responsible for, and ensuring that all records and data in the system are complete, accurate, timely, and relevant to accomplish a purpose of the agency as authorized by statute or Executive Order of the President.
- Collaborating with the Bureau/Office Privacy Officer to prepare documentation required by the Privacy Act, including notices of new, altered or terminated system of records for publication in the *Federal Register*, and reviewing each system of records notice annually to ensure it accurately describes the system of records.
- Receiving, evaluating, and granting or denying, as appropriate, requests by individuals for notification of, access to, and disclosure of records in the system.
- Receiving, evaluating and granting or denying, as appropriate, individuals' petitions to amend records in the system.
- Maintaining an accounting for disclosures from a Privacy Act system outside DOI and ensuring all recipients of records are informed when those records have been amended.
- Monitoring a contractor's compliance with Privacy Act requirements for systems of records maintained by the contractor on behalf of DOI.
- Formulating and maintaining records retention and disposal schedules, in consultation with the Bureau/Office Records Officer.
- Working with the Information System Owner and the Information System Security Officer to complete a PIA for any information system that collects or maintains Privacy Act information, and to ensure appropriate management, operational, physical, administrative, and technical safeguards are in place to prevent unauthorized disclosure or alteration of information in the system.

4.3 Information System Security Officer

An Information System Security Officer (ISSO) is appointed by an Information System Owner to ensure implementation of system-level security controls and to maintain system documentation. The ISSO is responsible for collaborating with the Information System Owner

to develop, implement, and manage corrective action plans for all systems they own and operate, and to develop a Plan of Actions and Milestones (POA&M) when necessary. The duties of the ISSO are very important and must be considered when an assignment is made by the Information System Owner as both Federal Information Security Management Act of 2002 (FISMA) and OMB policy require that Federal information systems employ effective security controls necessary for the protection of information. The ISSO has certain responsibilities for ensuring that operational security is maintained and that Federal and agency information security requirements are met. The ISSO works closely with the Information System Owner to manage the technical requirements of the system's security operations. The ISSO must review the PIA to ensure privacy risks were properly assessed and appropriate security controls were implemented to mitigate risks and protect privacy data.

The ISSO also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system, and must have the detailed knowledge and expertise required to manage the daily security aspects of an information system. ISSO responsibilities include, but are not limited to:

- Physical and environmental protection
- Managing and enforcing access restrictions and personnel security
- Reporting and handling privacy and security incidents
- Assisting in the development of privacy and security procedures
- Ensuring compliance with privacy and security procedures
- Monitoring the system and its environment of operation
- Developing and updating the System Security Plan (SSP)
- Managing and controlling changes to the system
- Assessing the security impact of those changes.

4.4 Chief Information Security Officer

The Chief Information Security Officer (CISO) is responsible for coordinating, developing, and implementing an information security program, and manages the security state of organizational information systems through security authorization processes. CISOs ensure that IT systems develop and maintain a complete A&A, and develop POA&Ms to document remedial actions and adequately respond to operational risks. The Bureau/Office CISO (BCISO) works closely with the appropriate privacy and security staff in the program offices to review, evaluate and recommend information security and privacy measures and safeguards to protect information from the loss, theft, misuse, unauthorized access, destruction, and unauthorized modification or disclosure whether accidental or intentional.

4.5 Records Officer

The Bureau/Office Records Officer is responsible for collaborating with the Information System Owner and Privacy Act System Manager to identify or develop records retention schedules with approval by the National Archives and Records Administration (NARA) for Federal records maintained within the system. The Bureau/Office Records Officer provides guidance to the Information System Owner on the management of records, the appropriate records retention and destruction schedules, and approved disposition methods.

It is important to collaborate on records requirements at an early stage of development as any system that contains Federal records that does not have a NARA approved records retention schedule must maintain those records permanently pending approval of the proposed records schedule by NARA.

Note that the Information System Owner needs to secure the information and assure its accuracy and integrity, so any proposed records schedule should align with the stated purpose and mission of the system. To protect individual privacy when developing records schedules, Bureau/Office Records Officers and Information System Owners should consider that PII only be retained for the minimum amount of time necessary to meet the requirements of the Federal Records Act.

4.6 Information Collection Clearance Officer

The Information Collection Clearance Officer (ICCO) is responsible for ensuring that all Bureau/Office information collection activities adhere to the requirements of the Paperwork Reduction Act of 1995 (PRA), OMB directives, and other applicable legislation. The ICCO provides technical assistance, guidance, advice, and training to Information System Owners, Privacy Act System Managers, and other Bureau/Office personnel to ensure compliance with OMB directives and the PRA.

The ICCO is responsible for establishing procedures for the systematic review of existing and proposed information collection requirements. The E-Government Act requires agencies to conduct a PIA on any new collection of information from ten (10) or more members of the public using information technology. The ICCO collaborates with Information System Owners, Privacy Act System Managers, and Bureau/Office Privacy Officers to review PIA requirements for new information collections and obtain OMB approval to collect the information.

4.7 Privacy Officer

The Privacy Officer is responsible for managing and overseeing privacy activities to ensure compliance with Federal privacy laws and policies. The Privacy Officer implements privacy policy, provides guidance, evaluates Bureau/Office programs, systems and initiatives for

potential privacy implications, and provides strategies to mitigate or reduce privacy risk. The Privacy Officer collaborates with Bureau/Office personnel, Information System Owners, and program managers to ensure privacy considerations are addressed when planning, developing or updating programs, systems or initiatives in order to protect individual privacy and ensure compliance with applicable privacy laws and regulations.

The Privacy Officer is responsible for supporting the Information System Owner in the development of the PIA to ensure it is accurate and complete, and adequately identifies and addresses privacy risks. The Privacy Officer reviews the PIA to ensure the appropriate privacy and security safeguards are implemented, records retention requirements are addressed, and published Privacy Act SORNs are identified for systems that contain Privacy Act records. The Privacy Officer maintains an inventory of approved PIAs, ensures PIAs are posted in CSAM and on the DOI Privacy Impact Assessment website as required, and assists in the completion of quarterly and annual FISMA reports for PIAs. Privacy Officer responsibilities include, but are not limited to:

- Administering the Privacy Program within Bureaus/Offices and implementing DOI privacy policies, procedures, standards, and guidelines.
- Identifying Privacy Act systems of records and working closely with Privacy Act System Managers, Information System Owners, and other officials to ensure compliance with the provisions of the Privacy Act, the E-Government Act, OMB mandates and DOI privacy policy.
- Reviewing proposed PIAs to confirm that privacy implications have been identified and evaluated to protect individual privacy while meeting information requirements necessary to meet DOI's mission, in accordance with the E-Government Act, OMB mandates and DOI policy.
- Reviewing and assessing privacy controls to ensure adequate safeguards are employed to protect PII, and to demonstrate compliance with Federal privacy requirements.
- Developing and coordinating documentation required by the Privacy Act, including notices of new, altered or terminated system of records for publication in the *Federal Register*, and reviewing system of records notices annually to determine necessary revisions.
- Overseeing Privacy Act System Managers' activities to ensure all privacy-related, statutory, regulatory, and DOI requirements are met.
- Providing privacy training and promoting awareness of employees' responsibility to protect personally identifiable information (PII).

4.8 Reviewing Official

The Reviewing Official is responsible for reviewing and approving PIAs to ensure that the requirements of the E-Government Act, OMB M-03-22, and DOI policy have been met. For Department-wide PIAs, this is the DOI Chief Information Officer (CIO)/SAOP. For Bureau/Office level PIAs, this is the Bureau/Office Assistant Director for Information Resources (ADIR). The Reviewing Official ensures PIAs adequately assess the privacy and security risks associated with the use of information systems and that remedial action is taken against any privacy deficiencies identified. A Reviewing Official cannot be an official who is responsible for the development, procurement, or management of the system.

Section 5.0 - Completing a PIA

5.1 DI-4001 PIA Form

The DI-4001 PIA form in Appendix A is an automated PIA form that has been developed for Departmental consistency and ease of use. All PIAs completed after the effective date of this amended Guidance must be in the DI-4001 PIA format. Use of the DI-4001 PIA form eliminates inconsistency in Department PIAs and simplifies the PIA completion and approval process. The DI-4001 PIA form includes specific questions designed to assess privacy risks and inform the public on how DOI collects, maintains, uses and safeguards PII. The questions in the PIA form are included in Section 6.0 below to provide additional guidance in responding to the questions in the PIA form.

The DI-4001 PIA form has an automated workflow and approval process with electronic signature capability, and is available to all Department personnel on the Enterprise Forms System (EFS) portal, https://eforms.doi.gov/, a cloud-based solution that automates internal and external Departmental, Bureau and Office forms. An automated PIA workflow is incorporated into the EFS to enable users to complete and submit PIA forms directly to the required individuals. The DI-4001 PIA allows for a streamlined PIA approval process, an improved efficient method for completing the PIA form, and immediate access to resources and tips.

5.2 Privacy Controls

NIST SP 800-53 Rev. 4 requires Federal agencies to implement privacy controls for information systems to ensure the protection and proper handling of PII and provides a structured set of controls for protecting privacy during the information life cycle. Privacy controls demonstrate the administrative, technical, and physical safeguards employed within organizations to protect PII and are applicable to all federal information systems, including national security systems consistent with the appropriate governing authorities. Information systems or program activities that do not involve the collection and use of PII may nevertheless raise privacy concerns that

have associated risks to individual privacy. These privacy controls may also be applied to those systems or activities to analyze the privacy risk and mitigate any such risk as necessary.

Privacy controls may vary dependent on mission or business needs of the organization based on legal authorities and obligations, and can be tailored to meet defined and specific needs for the particular mission/business functions. In many cases, privacy controls overlap with security controls to provide the fundamental information protection for confidentiality, integrity, and availability within information systems, which is essential for strong and effective privacy.

The SAOP has the final authority for the selection, implementation, and assessment of privacy controls as indicated in NIST SP 800-53. As such, the SAOP provides final approval for adequacy of the privacy controls selected and implemented for information systems, which is required for the issuance of an ATO. This approval is demonstrated by the PIA process, and is based on a determination of risk to the organization and to individuals, and an assessment of the privacy controls and safeguards implemented to mitigate any risk identified as appropriate.

The PIA is a requirement for the A&A process so it is important to conduct PIAs early in the information system life cycle to demonstrate that privacy risks are identified and addressed and ensure compliance with privacy and security policy. PIAs can effectively document that privacy controls are implemented as appropriate to satisfy the privacy requirements set forth in the Privacy Act of 1974, the E-Government Act, OMB privacy-related policies, and NIST standards. It is important that Information System Owners, Information System Security Officers, Authorizing Officials, Chief Information Security Officers, and other agency officials involved in risk management decisions, consult with the appropriate privacy officials at the earliest stages of system procurement or development to ensure privacy controls are implemented, and that they are appropriately identified and documented during the PIA process.

Identifying privacy controls during the PIA process will allow DOI to meet and demonstrate compliance with Federal privacy requirements and standards. Protecting the privacy of individuals and the PII that is collected, used, maintained, shared, and disposed of by programs and information systems depends on the safeguards and controls employed within the information systems or programs. The guidance in Section 6.0 includes recommendations for privacy controls that may be pertinent to the questions in the DI-4001 PIA form. The recommendations are not all inclusive, but are meant to provide guidance for identifying and assessing the controls and safeguards implemented for each information system or program. It is important that PIAs clearly identify any privacy controls implemented, and demonstrate that they are correctly implemented, are effective, and that they meet the standards for specific controls as appropriate. Note that there may be many other related privacy and security controls that apply to each question in the assessment, and personnel should not limit the controls documented during the PIA process to those specifically identified as recommendations in Section 6 of this

Guide. Personnel should review NIST SP 800-53 Rev. 4 for a full description of security and privacy controls, and specifically Appendix J for guidance on implementing privacy controls.

5.3 Guidelines for Completing a PIA

PIAs should be clear, unambiguous, and understandable to the general public. The length and breadth of a PIA will vary by the size and complexity of the program or system. Any system or new collection that processes PII should be able to demonstrate that an in-depth analysis was conducted to ensure that privacy protections were built into the system.

- Use Plain English. The PIA should be written in a manner that allows the public to understand the activities being described. Do not use overly technical language; instead use words or phrases that are readily known to the average person.
- Be detailed. Remember the purpose of the PIA. The PIA should be written with sufficient detail to permit the Privacy Office to analyze the privacy risks and mitigation steps.
- Answer all questions. If a particular question is not applicable please explain why it is not applicable, do not merely state "Not Applicable" – this will cause the PIA to be returned for further clarification.
- Correct simple errors. PIAs should be free of spelling and grammatical errors and written in active voice rather than passive voice. PIAs are published on the Department's PIA website.
- Explain Acronyms. Spell out each acronym the first time it is used in the document. For example: Office of Management and Budget (OMB).
- Define technical terms or references. Provide explanations if necessary. Keep in mind that readers may not understand technical terms when they are first used.
- Cite legal references and other previously published documents. Reference other systems, programs, or documents, and provide explanations in order for the public to gain a complete understanding of the context of the program or system. Use the complete name of referenced documents and provide a citation, and if possible a very brief description of the document type (e.g., system of records notice, statute, final or proposed rule). This allows the public the opportunity to understand and investigate the referenced document.

Section 6.0 - Contents of a PIA

6.1 General System Information

A. Is a PIA required?

This is a threshold question. Does the system collect, maintain, use or disseminate information about individuals? Indicate whether the system contains information about members of the general public, Federal employees, contractors, or volunteers; or if the system does not contain any information that is identifiable to individuals (e.g., statistical, geographic, financial). DOI policy requires that a PIA be completed for all systems. This threshold question, along with the other questions in Section 1 of the DI-4001 PIA form, helps determine whether the remaining section of the DI-4001 PIA form must be completed. For example, some systems may contain computer code or process information that is not in human readable format, and does not contain any information identifiable to individuals.

Note that if information on individuals 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, requires that those agencies that collect, use, or disseminate geographic information and/or carry out related spatial data activities also comply with Federal government law and policy on privacy protection (see 2.a. and 8.a.7 of the Circular at http://www.whitehouse.gov/omb/circulars_a016_rev/).

This question is directly related to privacy control AR-2, Privacy Impact and Risk Assessment, which requires organizations to conduct PIAs and assess privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

B. What is the purpose of the system?

Describe the purpose of the system, technology, project or other collection and how it relates to the program office's and Department's mission. Include the context and background necessary to understand the purpose of the project, the name of the program office conducting the PIA and the name of the system, technology, project or collection being assessed.

This question is directly related to privacy control AP-2, Purpose Specification, which requires organizations to clearly describe the specific purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and privacy compliance documentation.

C. What is the legal authority?

List all statutory and regulatory authority and Executive Orders for maintenance of the system or information collection to meet an official program mission or goal. Explain how the statutory and regulatory authority permits collection and use of the information. If there is an existing Privacy Act SORN for the system, then the response should reflect the

information provided in the authority section of the notice. Do not cite the Privacy Act of 1974 as the authority for the collection or maintenance of information.

This question is directly related to privacy controls AP-1, Authority to Collect, and UL-1, Internal Use.

- AP-1, Authority to Collect, requires organizations to determine the legal authority of the program or activity that permits the collection, use, maintenance and sharing of PII, and to document that authority in privacy compliance documentation.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

D. Why is the PIA being completed or modified?

Explain why the PIA is being conducted. Include a description of the function of the system, technology, project or collection and how it collects information and the reason why the PIA is required. For example, a new system is being developed, the system is being significantly modified, or two systems are being merged together.

This question is related to privacy controls AP-2, Purpose Specification, and AR-7, Privacy-Enhanced System Design and Development.

- AP-2, Purpose Specification, requires organizations to clearly describe the specific purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and privacy compliance documentation.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems and employ system capabilities to automate privacy controls on the collection, use, and sharing of PII to mitigate privacy risks and support privacy protections. This includes regular monitoring of system use and conducting periodic reviews for changes and updates to the system and to privacy compliance documentation as necessary.

E. Is the information system registered in CSAM?

If the system is registered in the Cyber Security Assessment and Management (CSAM) tool, provide the System Security Plan (SSP) name if one has been completed for the information system(s). This may be obtained from the designated Information System Security Officer

(ISSO). The completed PIA, associated SORNs, and any other supporting artifacts must be entered into CSAM for each registered system or application.

This question is related to privacy controls AR-1, Governance and Privacy Program; AR-4, Privacy Monitoring and Auditing; AR-6, Privacy Reporting; and UL-1, Internal Use.

- AR-1, Governance and Privacy Program, requires organizations to develop and implement policies and procedures that govern privacy and security controls for programs, information systems, or technologies involving PII; demonstrate accountability for the protection of PII; and monitor compliance with privacy controls and privacy operations. CSAM is the official repository for DOI information systems and for the privacy and security compliance documentation associated with those systems. Accurate and complete information and supporting compliance documentation for the systems in CSAM is crucial to the privacy governance process and for accurate privacy reporting.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take appropriate corrective actions.

- AR-6, Privacy Reporting, requires organizations to develop reports to OMB, Congress, and other oversight entities to demonstrate accountability with statutory and regulatory privacy program mandates to promote accountability and transparency, and help determine performance and progress in meeting compliance requirements. These reports include the annual SAOP report to Congress as part of the FISMA report, annual reports to Congress on agency activities in the information sharing environment, and annual reports to OMB on agency implementation of the provisions of the E-Government Act.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

Identify all minor applications or subsystems hosted on the system, the purpose of the application(s), and describe any PII that may be contained in each application. For General Support Systems (GSS) that host major applications, minor applications, or other subsystems, be sure to include all such systems hosted and describe the purposes and types of PII, if any.

Privacy risks must adequately be addressed for each hosted application or subsystem in the GSS PIA or in a separate PIA conducted specifically for the hosted application or subsystem. In both cases, 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.

This question is related to privacy controls AR-1, Governance and Privacy Program, and AR-4, Privacy Monitoring and Auditing.

- AR-1, Governance and Privacy Program, requires organizations to develop and implement policies and procedures that govern privacy and security controls for programs, information systems, or technologies involving PII; demonstrate accountability for the protection of PII; and monitor compliance with privacy controls and privacy operations. The applications and subsystems identified in the PIA should correlate to those in CSAM, the official repository for DOI information systems and for the privacy and security compliance documentation associated with those systems. It is very important that accurate and complete information regarding minor applications, subsystems, boundaries, and the supporting compliance documentation for them is updated in CSAM, for the privacy governance process and for accurate privacy reporting.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take appropriate corrective actions.

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

For all collections of PII where the information is retrieved by a name or other personal identifier, the Privacy Act requires that the agency publish a SORN in the *Federal Register*. Information System Owners must collaborate with Bureau/Office Privacy Officers to identify, or develop and publish a SORN. If an existing SORN applies to the collection of information, include the SORN identifier and the *Federal Register* citation. The Privacy Act requires that amendments to an existing system must also be addressed in a *Federal Register* notice (see 383 Departmental Manual 5.3, "Reports on New or Altered Systems").

If the system requires development of a new SORN, the SORN must be published in the *Federal Register* before the system can operate. The Privacy Act contains criminal penalties for operating a system of records without publishing a SORN. Any officer or employee who

knowingly and willfully maintains a system of records 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, and be subject to disciplinary action.

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. Provide an explanation if the system does not require a SORN.

This question is directly related to privacy control TR-2, System of Records Notices and Privacy Act Statements, which requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals, and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

H. Does this information system or electronic collection require an OMB Control Number?

The Paperwork Reduction Act of 1995 establishes requirements for collecting the same information from 10 or more members of the public. Any information collection from members of the public may require OMB approval. Consult your Bureau/Office Information Collection Clearance Officer to ensure that you have OMB approval, or to determine whether you need to obtain an OMB approval to collect the information.

If the system information is covered by the Paperwork Reduction Act, provide the OMB Control Number for the collection. Be sure to include all applicable OMB Control numbers.

This question is related to privacy controls AR-2, Privacy Impact and Risk Assessment, and DI-1, Data Quality.

- AR-2, Privacy Impact and Risk Assessment, requires organizations to conduct PIAs and assess privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII. This requirement applies to information collections as the E-Government Act requires agencies to conduct a PIA on any new collection of information from ten (10) or more members of the public using information technology. Information System Owners, Privacy Act System Managers, Bureau/Office Privacy Officers must collaborate with the ICCO to review PIA requirements for new information collections and obtain OMB approval to collect the information as part of the information collection clearance process.

- DI-1, Data Quality, requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created; collect PII directly from individuals to the greatest extent practicable; check and correct any inaccurate or outdated PII used by programs of information systems; and issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. This may include verifying data as it is collected or entered into systems, verifying sources of data if not collected directly from the individual, and reviewing and updating PII holdings regularly to ensure accuracy, relevance, and completeness.

6.2 Summary of System Data

A. What PII will be collected?

Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. This could include: name, address, telephone number, SSN, Tribal enrollment number, date of birth, e-mail address, facsimile number, mother's maiden name, nationality, country of citizenship, spouse or dependent information, credit card number, bank account number, any other account numbers, vehicle license plate numbers, medical records, civil or criminal history information, education records, biometric identifiers, photographic facial image, or any other unique identifying number or characteristic. If the system creates new information (for example, an analysis or report) describe how this is done and the purpose of that information.

This question is related to privacy control SE-1, Inventory of Personally Identifiable Information, which requires organizations to maintain an inventory of programs and information systems identified as collecting, using, maintaining, or sharing PII, and to provide updated PII inventories to appropriate information security official to support information security requirements for new or modified information systems containing PII. This allows organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII and to mitigate the risk of PII

exposure. Organizations should utilize PIAs and SORNs to identify information systems and programs that contain PII.

B. What is the source for the PII collected?

Indicate all sources of PII that will be collected. Information may be collected directly from an individual through a written form, website collection, or through interviews over the phone or in person. Information may also come from agency officials and employees, agency records, a computer readable extract from another system, or may be created within the system itself.

If information is being collected from sources other than the individual, such as an interface with other systems, systems of records, commercial data aggregators, or other agencies, list the source(s) and explain why information from sources other than the individual is required.

This question is related to privacy controls DI-1, Data Quality; IP-1, Consent; TR-1, Privacy Notice; and TR-2, System of Records Notices and Privacy Act Statements.

- DI-1, Data Quality, requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created; collect PII directly from individuals to the greatest extent practicable; check and correct any inaccurate or outdated PII used by programs of information systems; and issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. This may include verifying data as it is being collected or entered into systems, verifying sources of data if not collected directly from the individual, and reviewing and updating PII holdings regularly to ensure accuracy, relevance, and completeness.

- IP-1, Consent, requires organizations to provide a means for individuals to authorize the collection, use, and sharing of PII prior to its collection, and for individuals to understand the consequences of decisions to provide or decline the collection, use, and sharing of PII. Consent ensures that individuals can participate in the process of collection and using their PII and understand the potential risk to their privacy. Consent may include opt-in, where the individual takes affirmative action to allow the collection or use of PII, such as signing a form or clicking a radio button in agreement; opt-out, where individuals take action to prevent the collection or use of PII, such as individuals signing up for the Do-Not-Call Registry or taking steps to opt out of browser add-ons when visiting websites; or implied consent as appropriate, though implied consent is the least preferred method and should be limited to situations where behavior or failure to object indicates agreement (e.g., entering and

remaining in a facility where a Privacy Notice is posted advising individuals that they are being monitored via security cameras implies consent to video recording).

- TR-1, Privacy Notice, requires organizations to provide notice to the public and individuals regarding activities that impact individual privacy, including the authority for collecting PII; what PII is collected; whether the PII is shared with an external organization; how the agency handles the collection, use, sharing, and disposal of PII; any opportunity for the individual to consent to the collection and use of PII, and any consequences for consenting or not consenting; and how individuals can access and amend PII if necessary. This requirement applies whether or not the PII involved is maintained in a Privacy Act system of records. There are many ways an organization can provide notice to the public, including SORNs, PIAs, website Privacy Policy, Privacy Act Statements, and Privacy Notices directly related to information collections, web pages, or third-party website or applications.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

C. How will the information be collected?

Indicate all the formats or methods for collecting PII that will be used. For example, information may be collected through a written form, website collection, through interviews over the phone or in person, other agency officials and employees, agency records, computer readable extract from another system, interface with other Federal agency systems, or commercial data aggregators. If the system receives information from another system, such as a transfer of financial information or response to a background check, describe the system

from which the information originates, what information is received, how the information is used, and how the systems interface.

This question is related to privacy controls AR-7, Privacy-Enhanced System Design and Development; DI-1, Data Quality; TR-1, Privacy Notice; TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

- AR-7, Privacy-Enhanced System Design and Development, which relates information systems that employ technologies and system capabilities that automate privacy controls or protections on the collection, use, retention, and disclosure of PII. Include any processes for systems that provide or receive data feeds or updates or that interface with other systems.

- DI-1, Data Quality, requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created, and to collect PII directly from individuals to the greatest extent practicable.

- TR-1, Privacy Notice, requires organizations to provide notice to the public and individuals regarding activities that impact individual privacy, including the authority for collecting PII; what PII is collected; whether the PII is shared with an external organization; how the agency handles the collection, use, sharing, and disposal of PII; any opportunity for the individual to consent to the collection and use of PII, and any consequences for consenting or not consenting; and how individuals can access and amend PII if necessary. This requirement applies whether or not the PII involved is maintained in a Privacy Act system of records. There are many ways an organization can provide notice to the public, including SORNs, PIAs, website Privacy Policy, Privacy Act Statements, and Privacy Notices directly related to information collections, web pages, or third-party website or applications.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and

access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

D. What is the intended use of the PII collected?

Describe the intended uses of the PII collected and maintained in the system, and include an example that details the life cycle from collection to disposal of the PII. For systems with multiple uses, list each use of the information collected or maintained and provide a detailed explanation on how the data will be used. The intended use must be relevant to the purpose of the system. For Privacy Act systems, each use must be compatible with the published SORN.

This question is related to privacy controls AP-2, Purpose Specification; TR-1, Privacy Notice; TR-2, System of Records Notices and Privacy Act Statements; UL-1, Internal Use; and UL-2, Information Sharing with Third Parties.

- AP-2, Purpose Specification, which requires organizations to clearly describe the specific purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and privacy compliance documentation. The use of PII must be relevant to the purpose of the collection of the PII, and for Privacy Act systems, must be compatible with the SORN that covers the system. SORNs should be reviewed and updated when necessary to ensure uses of PII remains authorized and consistent with the Privacy Act and the SORN.

- TR-1, Privacy Notice, requires organizations to provide notice to the public and individuals regarding activities that impact individual privacy, including the authority for collecting PII; what PII is collected; whether the PII is shared with an external organization; how the agency handles the collection, use, sharing, and disposal of PII; any opportunity for the individual to consent to the collection and use of PII, and any consequences for consenting or not consenting; and how individuals can access and amend PII if necessary. This requirement applies whether or not the PII involved is maintained in a Privacy Act system of records. There are many ways an organization can provide notice to the public, including SORNs, PIAs, website Privacy Policy, Privacy Act Statements, and Privacy Notices directly related to information collections, web pages, or third-party website or applications.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

- UL-1, Internal Use, requires organizations to take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and the applicable published system of records notices.

- UL-2, Information Sharing with Third Parties, requires organizations to share PII only for authorized purposes in accordance with the disclosure requirements of the Privacy Act and any applicable system of records notice(s). Any such sharing with third parties should be described in a Memorandum of Understanding, Memorandum of Agreement, Computer Matching Agreement, or other similar agreements, and specifically describe the PII covered, how it may be used, and the safeguards applied to protect the information. The applicable PIA(s) and SORN(s) should be updated to address this information sharing. Also, note that there are other considerations related to the sharing of information with third parties. Are Computer Matching Agreements published? Is the information sharing with other partners in the information sharing environment (ISE), and subject to the ISE Privacy Guideline or other Federal mandates that govern the ISE? Any disclosure of Privacy Act records to a third party pursuant to a published routine use must be documented - organizations can use the DI-3710, Disclosure Accounting form for this purpose.

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

Indicate all the categories of parties both internal and external to DOI with whom PII will be shared. Identify other DOI offices with assigned roles and responsibilities within the system, or with whom information is shared, and describes how and why information is shared.

Identify other Federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared. Describe any routine information sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. Explain how the information is accessed and used, and provide details on any Memorandum of Understanding (MOU), contract or other agreement that governs the sharing of information in the system and whether there are limitations on re-dissemination. Note that information shared with external entities must be compatible with the purpose and use as stated in the applicable published SORN.

Describe how an accounting of disclosures made outside DOI is maintained. See the Privacy Act, 5 U.S.C. 552a (c) for requirements to account for records disclosed to external parties. The DI-3710 Disclosure Accounting form should be used to record the date, nature and purpose of each disclosure from a Privacy Act systems of records, and the name and address of the individual or agency to whom the disclosure is made.

This question is related to privacy controls AR-3, Privacy Requirements for Contractors and Service Providers; AR-8, Accounting of Disclosures; DI-2, Data Integrity and Data Integrity Board; TR-1, Privacy Notice; TR-2, System of Records Notices and Privacy Act Statements; UL-1, Internal Use; and UL-2, Information Sharing with Third Parties.

- AR-3, Privacy Requirements for Contractors and Service Providers, requires organizations to establish privacy roles, responsibilities, and access requirements for contractors and service providers, and to include privacy requirements in contracts and other acquisition-related documents. Contracts should include the required FAR clauses, as well as the required safeguards, privacy controls, and other provisions related to the handling, maintenance and processing of PII for information providers, information processors, and other organizations.

- AR-8, Accounting of Disclosures, requires organizations to keep an accurate accounting of disclosures of information held in each system of records under its control to ensure they are being properly maintained and provided to persons named in those records consistent with the Privacy Act and to retain them for the life of the record or five years after the disclosure is made, whichever is longer. These disclosures must be made available to the individual who is the subject of the record upon request. This requirement is outlined in DOI Privacy Act regulations at 43 CFR

2.232 and in 383 Departmental Manual 7.8. The Department has issued DI-3710, Disclosure Accounting form for this purpose.

- DI-2, Data Integrity and Data Integrity Board, requires organizations to document processes to ensure the integrity of PII through existing security controls; and to establish a Data Integrity Board to oversee and implement Computer Matching Agreements and to ensure those agreements comply with computer matching provisions of the Privacy Act.

- TR-1, Privacy Notice, requires organizations to provide notice to the public and individuals regarding activities that impact individual privacy, including the authority for collecting PII; what PII is collected; whether the PII is shared with an external organization; how the agency handles the collection, use, sharing, and disposal of PII; any opportunity for the individual to consent to the collection and use of PII, and any consequences for consenting or not consenting; and how individuals can access and amend PII if necessary. This requirement applies whether or not the PII involved is maintained in a Privacy Act system of records. There are many ways an organization can provide notice to the public, including SORNs, PIAs, website Privacy Policy, Privacy Act Statements, and Privacy Notices directly related to information collections, web pages, or third-party website or applications.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

- UL-2, Information Sharing with Third Parties, requires organizations to share PII only for authorized purposes in accordance with the disclosure requirements of the Privacy Act and any applicable system of records notice(s). Any such sharing with third parties should be described in a Memorandum of Understanding, Memorandum of Agreement, Computer Matching Agreement, or other similar agreements, and specifically describe the PII covered, how it may be used, and the safeguards applied to protect the information. The applicable PIA(s) and SORN(s) should be updated to address this information sharing. Also, note that there are other considerations related to the sharing of information with third parties. Are Computer Matching Agreements published? Is the information sharing with other partners in the ISE, and subject to the ISE Privacy Guideline or other Federal mandates that govern the ISE? Any disclosure of Privacy Act records to a third party pursuant to a published routine use must be documented - organizations can use the DI-3710, Disclosure Accounting form for this purpose.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

Indicate whether individuals have the opportunity to consent to specific uses of information collected or to decline to provide information, and whether the consequences of not providing information are included in the notice. Describe the process of how an individual may exercise the right to consent to particular uses or decline to provide information, or explain why individuals cannot provide or withhold consent. In some cases, notice may not be appropriate. Explain how providing direct notice to the individual at the time of collection would undermine or be inconsistent with the purpose of the collection.

This question is directly related to privacy control IP-1, Consent, which requires organizations to provide a means for individuals to authorize the collection, use, and sharing of PII prior to its collection, and for individuals to understand the consequences of decisions to provide or decline the collection, use, and sharing of PII. Consent ensures that individuals can participate in the process and understand the potential risk to their privacy. Consent may include opt-in, where the individual takes affirmative action to allow the collection or use of PII, such as signing a form or clicking a radio button in agreement; opt-out, where individuals take action to prevent the collection or use of PII, such as individuals registering for the Do-Not-Call Registry or taking steps to opt out of browser add-ons when visiting websites; or implied consent when appropriate, though implied consent is the least preferred method and should be limited to situations where behavior or failure to object indicates agreement (e.g., entering and remaining in a facility where a Privacy Notice is posted advising individuals that they are being monitored via security cameras implies consent to video recording).

Other related privacy controls include TR-1, Privacy Notice; TR-2, System of Records Notices and Privacy Act Statements; TR-3, Dissemination of Privacy Program Information; UL-1, Internal Use; and UL-2, Information Sharing with Third Parties.

- TR-1, Privacy Notice, requires organizations to provide notice to the public and individuals regarding activities that impact individual privacy, including the authority for collecting PII; what PII is collected; whether the PII is shared with an external organization; how the agency handles the collection, use, sharing, and disposal of PII; any opportunity for the individual to consent to the collection and use of PII, and any consequences for consenting or not consenting; and how individuals can access and amend PII if necessary. This requirement applies whether or not the PII involved is maintained in a Privacy Act system of records. There are many ways an organization can provide notice to the public, including SORNs, PIAs, website Privacy Policy, Privacy Act Statements, and Privacy Notices directly related to information collections, web pages, or third-party website or applications.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

- TR-3, Dissemination of Privacy Program Information, requires agencies to ensure its privacy practices are publically available on official websites and the public has access to PIAs, SORNs, privacy reports, and other information about its privacy activities. DOI publishes PIAs, SORNs, reports, policies, and other resources on the DOI Privacy Program website to provide information to the public on the privacy policies and practices of the Department. The DOI Privacy Policy for the Interior website also provides information to the public on the Department's privacy

practices. Organizations should include any resource or mechanism that provides notice to the public on privacy practices that may impact them so they may be informed and be able to participate in the decisions about the provision and use of their PII.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

- UL-2, Information Sharing with Third Parties, requires organizations to share PII only for authorized purposes in accordance with the disclosure requirements of the Privacy Act and any applicable system of records notice(s). Any such sharing with third parties should be described in a Memorandum of Understanding, Memorandum of Agreement, Computer Matching Agreement, or other similar agreements, and specifically describe the PII covered, how it may be used, and the safeguards applied to protect the information. The applicable PIA(s) and SORN(s) should be updated to address this information sharing. Also, note that there are other considerations related to the sharing of information with third parties. Are Computer Matching Agreements published? Is the information sharing with other partners in the ISE, and subject to the ISE Privacy Guideline or other Federal mandates that govern the ISE? Any disclosure of Privacy Act records to a third party pursuant to a published routine use must be documented - organizations can use the DI-3710, Disclosure Accounting form for this purpose.

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

Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, notice to individuals may include Privacy Act Statements, posted Privacy Notices, a Privacy Policy, and published SORNs and PIAs.

If possible, provide a copy of the Privacy Act Statement, Privacy Notice, a link to the applicable Privacy Policy, procedure or PIA(s), or reference the SORN *Federal Register* citation (e.g., XX FR XXXX, Date) for review. Describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).

This question is directly related to privacy controls TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements.

- TR-1, Privacy Notice, requires organizations to provide notice to the public and individuals regarding activities that impact individual privacy, including the authority for collecting PII; what PII is collected; whether the PII is shared with an external organization; how the agency handles the collection, use, sharing, and disposal of PII; any opportunity for the individual to consent to the collection and use of PII, and any consequences for consenting or not consenting; and how individuals can access and amend PII if necessary. This requirement applies whether or not the PII involved is maintained in a Privacy Act system of records. There are many ways an organization can provide notice to the public, including SORNs, PIAs, website Privacy Policy, Privacy Act Statements, and Privacy Notices directly related to information collections, web pages, or third-party website or applications.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

H. How will data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Describe how data is retrieved from the system. For example, is data retrieved manually or via reports generated automatically? Is specific retrieval identifiers used or does the system use key word searches? Be sure to list the identifiers that will be used to retrieve data (e.g., name, case number, Tribal Identification Number, subject matter, date, etc.).

This question is related to privacy controls TR-2, System of Records Notices and Privacy Act Statements, and UL-1, Internal Use.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

I. Will reports be produced on individuals?

Indicate whether reports will be produced on individuals. Provide an explanation on the purpose of the reports generated, how the reports will be used, what data will be included in the reports, who the reports will be shared with, and who will have access to the reports. Many information systems have the capability to produce reports on the data contained in the system. Also, systems that have audit functions can generate reports on user actions. For example, audit logs can be generated that show the username, date and time of system access, number of failed attempts, files accessed by the user, etc. Be sure to include any such reports generated by the system.

This question is related to privacy controls AR-4, Privacy Monitoring and Auditing, and UL-1, Internal Use.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

6.3 Attributes of System Data

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

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.

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)).

This question is related to privacy controls DI-1, Data Quality; DM-1, Minimization of Personally Identifiable Information; and IP-3, Redress.

- DI-1, Data Quality, requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created; collect PII directly from individuals to the greatest extent practicable; check and correct any inaccurate or outdated PII used by programs of information systems; and issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. This may include verifying data as it is collected or entered into systems, verifying sources of data if not collected directly from the individual, and reviewing and updating PII holdings regularly to ensure accuracy, relevance, and completeness.

- DM-1, Minimization of Personally Identifiable Information, requires organizations to identify the minimum PII elements that are relevant and necessary for the legally authorized purpose of collection; limit the collection and retention of PII; and conduct periodic evaluations to ensure that PII identified in the notice is collected and retained.

Organizations should limit and reduce the use of PII where feasible to protect individual privacy, and conduct periodic reviews of PII inventories to ensure the collection and maintenance of the PII is necessary and appropriate, as well as accurate, timely, and complete.

- IP-3, Redress, which requires organizations to provide a process for individuals to correct or amend inaccurate PII maintained by the organization. This facilitates accuracy and demonstrates organizational commitment to data quality, and is especially important in areas where inaccuracy of data may result in negative determinations about individuals or a denial of benefits or services. In some cases, inaccurate data shared with partners may also have a negative impact on the privacy, civil rights, and civil liberties of affected individuals. It is important that the organization have an established process for assessing requests for redress, disseminating any corrections or amendments made to the PII maintained and shared with other authorized users of the PII, such as external third parties or partners in the ISE.

B. How will data be checked for completeness?

Describe the procedures to ensure data is checked for completeness. To the extent practical, PII should be checked for completeness to ensure accuracy within the context of the use of the data.

This question is related to DI-1, Data Quality, which requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created; collect PII directly from individuals to the greatest extent practicable; check and correct any inaccurate or outdated PII used by programs of information systems; and issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. This may include verifying data as it is collected or entered into systems, verifying sources of data if not collected directly from the individual, and reviewing and updating PII holdings regularly to ensure accuracy, relevance, and completeness.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Describe the steps or procedures taken to ensure the data is current and not out-of-date. Where are they documented? For example, are they outlined in standard operating procedures or data models? Data that is not current also affects the relevancy and accuracy of the data. This is particularly true with data warehousing. A data warehouse is a repository of an organization's electronically stored data and is designed to facilitate reporting and

analysis of its data. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.

This question is related to DI-1, Data Quality, which requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created; collect PII directly from individuals to the greatest extent practicable; check and correct any inaccurate or outdated PII used by programs of information systems; and issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. This may include verifying data as it is collected or entered into systems, verifying sources of data if not collected directly from the individual, and reviewing and updating PII holdings regularly to ensure accuracy, relevance, and completeness.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Is there a records retention schedule approved by the National Archives and Records Administration (NARA) for records in the system? Information System Owners must consult with Bureau/Office Records Officers early in the development process to ensure that appropriate retention and destruction schedules are identified, or to develop a records retention schedule for the records contained in the information system. New records retention schedules must be submitted to NARA for official approval.

Identify all applicable records retention schedules or explain at what development stage the proposed records retention schedule is in. Some systems may not require the development of a new retention schedule; however, any system that contains Federal records that does not have a NARA approved records retention schedule must maintain those records permanently pending approval of the proposed records schedule by NARA.

Describe the specific types of information the system retains and explain whether all the information is retained or if there are specific subsets of information that are retained. Also describe if subsets of information are deleted and how and when they are deleted. Be sure to include applicable records retention schedules for different types of information or subsets of information.

Note that the agency needs to secure the information and assure its accuracy and integrity so any proposed records schedule should align with the stated purpose and mission of the system, and PII should only be retained for the minimum amount of time necessary to meet DOI's mission and the requirements of the Federal Records Act.

This question is directly related to privacy control DM-2, Data Retention and Disposal, which requires organizations to retain collections of PII to fulfill the purpose identified in the

notice or as required by law in support of operational needs. PII should be retained in accordance with a NARA-approved records retention schedules and disposed of approved methods to ensure secure deletion or destruction of the PII, including shredding, erasing, and anonymizing the PII, in a manner that prevents loss, theft, misuse, or unauthorized access.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This may be obtained from records retention schedules, the Departmental Manual, Bureau/Office records management policies, or standard operating procedures.

This question is directly related to privacy control DM-2, Data Retention and Disposal, which requires organizations to retain collections of PII to fulfill the purpose identified in the notice or as required by law in support of operational needs. PII should be retained in accordance with a NARA-approved records retention schedules and disposed of approved methods to ensure secure deletion or destruction of the PII, including shredding, erasing, and anonymizing the PII, in a manner that prevents loss, theft, misuse, or unauthorized access.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

Describe and analyze the major potential privacy risks identified and discuss the overall impact on the privacy of employees or individuals. Include a description of how the program office has taken steps to protect individual privacy and mitigate the privacy risks. Provide an example of how information is handled at each stage of the information life cycle.

Also, discuss privacy risks associated with the sharing of information outside of the Department and how those risks were mitigated. Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department.

This question is related to privacy controls AR-2, Privacy Impact and Risk Assessment; AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; DM-1, Minimization of Personally Identifiable Information; DM-2, Data Retention and Disposal; DM-3, Minimization of PII Used in Testing, Training, and Research; SE-1, Inventory of Personally Identifiable Information; UL-1, Internal Use, and UL-2, Information Sharing with Third Parties.

- AR-2, Privacy Impact and Risk Assessment, requires organizations to conduct PIAs and assess privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

- AR-4, Privacy Monitoring and Auditing, organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems that employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII and to conduct periodic reviews of information systems.

- DM-1, Minimization of Personally Identifiable Information, requires organizations to identify the minimum PII elements that are relevant and necessary for the legally authorized purpose of collection; limit the collection and retention of PII; and conduct periodic evaluations to ensure that PII identified in the notice is collected and retained. Organizations should limit and reduce the use of PII where feasible to protect individual privacy, and conduct periodic reviews of PII inventories to ensure the collection and maintenance of the PII is necessary and appropriate, as well as accurate, timely, and complete.

- DM-2, Data Retention and Disposal, requires organizations to retain collections of PII to fulfill the purpose identified in the notice or as required by law in support of operational needs. PII should be retained in accordance with a NARA-approved records retention schedules and disposed of approved methods to ensure secure deletion or destruction of the PII, including shredding, erasing, and anonymizing the PII, in a manner that prevents loss, theft, misuse, or unauthorized access.

- DM-3, Minimization of PII Used in Testing, Training, and Research, requires organizations to develop policies and procedures that minimize the use of PII and implement controls to protect PII for testing, training, and research. If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes.

- SE-1, Inventory of Personally Identifiable Information, requires organizations to maintain an inventory of programs and information systems identified as collecting, using, maintaining, or sharing PII, and to provide updated PII inventories to appropriate information security official to support information security requirements

for new or modified information systems containing PII. This allows organizations to implement effective administrative, technical, and physical security policies and procedures to protect PII and to mitigate the risk of PII exposure. Organizations should utilize PIAs and SORNs to identify information systems and programs that contain PII.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

- UL-2, Information Sharing with Third Parties, requires organizations to share PII only for authorized purposes in accordance with the disclosure requirements of the Privacy Act and any applicable system of records notice(s). Any such sharing with third parties should be described in a Memorandum of Understanding, Memorandum of Agreement, Computer Matching Agreement, or other similar agreements, and specifically describe the PII covered, how it may be used, and the safeguards applied to protect the information. The applicable PIA(s) and SORN(s) should be updated to address this information sharing. Also, note that there are other considerations related to the sharing of information with third parties. Are Computer Matching Agreements published? Is the information sharing with other partners in the ISE, and subject to the ISE Privacy Guideline or other Federal mandates that govern the ISE? Any disclosure of Privacy Act records to a third party pursuant to a published routine use must be documented - organizations can use the DI-3710, Disclosure Accounting form for this purpose.

6.4 PIA Risk Review

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

Describe how the use of the system or information collection relates to the purpose of the underlying mission of the organization. Is the information directly relevant and necessary to accomplish the specific purposes of the system?

For Privacy Act systems, the Privacy Act at 5 U.S.C. 552a(e)(1) requires that each agency shall maintain in its records only such information about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by Executive Order of the President.

This question is related to privacy controls AP-2, Purpose Specification; DM-1, Minimization of Personally Identifiable Information; TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

- AP-2, Purpose Specification, which requires organizations to clearly describe the specific purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and privacy compliance documentation.

- DM-1, Minimization of Personally Identifiable Information, requires organizations to identify the minimum PII elements that are relevant and necessary for the legally authorized purpose of collection; limit the collection and retention of PII; and conduct periodic evaluations to ensure that PII identified in the notice is collected and retained. Organizations should limit and reduce the use of PII where feasible to protect individual privacy, and conduct periodic reviews of PII inventories to ensure the collection and maintenance of the PII is necessary and appropriate, as well as accurate, timely, and complete.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

Does the technology create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? Is data aggregated in a way that will permit system users to easily draw new conclusions or inferences about an individual? Electronic systems can sift through large amounts of information in response to user inquiry or programmed functions, or perform complex analytical tasks resulting in other types of data, matching, relational or pattern analysis, or reporting. Discuss the results generated by these uses and include an explanation on how the results are generated, whether by the information system or manually by authorized personnel. Explain the purpose and what will be done with the newly derived data.

Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information to form additional information that is usually different from the original source of information. Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.

This question is related to privacy controls AP-2, Purpose Specification; AR-2, Privacy Impact and Risk Assessment; and UL-1, Internal Use.

- AP-2, Purpose Specification, requires organizations to clearly describe the specific purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and privacy compliance documentation. The use of PII must be relevant to the purpose of the collection of the PII, and for Privacy Act systems, must be compatible with the SORN that covers the system. SORNs should be reviewed and updated when necessary to ensure uses of PII remains authorized and consistent with the Privacy Act and the SORN.

- AR-2, Privacy Impact and Risk Assessment, requires organizations to conduct PIAs and assess privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

Will the results be placed in the individual's record? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

This question is related to privacy controls AP-2, Purpose Specification; AR-2, Privacy Impact and Risk Assessment; DI-1, Data Quality; DM-1, Minimization of Personally Identifiable Information; TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

- AP-2, Purpose Specification, requires organizations to clearly describe the specific purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and privacy compliance documentation. The use of PII must be relevant to the purpose of the collection of the PII, and for Privacy Act systems, must be

compatible with the SORN that covers the system. SORNs should be reviewed and updated when necessary to ensure uses of PII remains authorized and consistent with the Privacy Act and the SORN.

- AR-2, Privacy Impact and Risk Assessment, requires organizations to conduct PIAs and assess privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

- DI-1, Data Quality, requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created; collect PII directly from individuals to the greatest extent practicable; check and correct any inaccurate or outdated PII used by programs of information systems; and issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. This may include verifying data as it is collected or entered into systems, verifying sources of data if not collected directly from the individual, and reviewing and updating PII holdings regularly to ensure accuracy, relevance, and completeness.

- DM-1, Minimization of Personally Identifiable Information, requires organizations to identify the minimum PII elements that are relevant and necessary for the legally authorized purpose of collection; limit the collection and retention of PII; and conduct periodic evaluations to ensure that PII identified in the notice is collected and retained. Organizations should limit and reduce the use of PII where feasible to protect individual privacy, and conduct periodic reviews of PII inventories to ensure the collection and maintenance of the PII is necessary and appropriate, as well as accurate, timely, and complete.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other

provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

Will the new data be used to make determinations about individuals or will it have any other effect on the subject individuals? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

This question is related to privacy controls AP-2, Purpose Specification; AR-2, Privacy Impact and Risk Assessment; DI-1, Data Quality; DM-1, Minimization of Personally Identifiable Information; TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

- AP-2, Purpose Specification, requires organizations to clearly describe the specific purpose(s) for which PII is collected, used, maintained, and shared in its privacy notices and privacy compliance documentation. The use of PII must be relevant to the purpose of the collection of the PII, and for Privacy Act systems, must be compatible with the SORN that covers the system. SORNs should be reviewed and updated when necessary to ensure uses of PII remains authorized and consistent with the Privacy Act and the SORN.

- AR-2, Privacy Impact and Risk Assessment, requires organizations to conduct PIAs and assess privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

- DI-1, Data Quality, requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created; collect PII directly from individuals to the greatest extent practicable; check and correct any inaccurate or outdated PII used by programs of information systems; and issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. This may include verifying data as it is collected or entered into systems, verifying sources of data if not collected directly from the individual, and reviewing and updating PII holdings regularly to ensure accuracy, relevance, and completeness.

- DM-1, Minimization of Personally Identifiable Information, requires organizations to identify the minimum PII elements that are relevant and necessary for the legally authorized purpose of collection; limit the collection and retention of PII; and conduct periodic evaluations to ensure that PII identified in the notice is collected and retained. Organizations should limit and reduce the use of PII where feasible to protect individual privacy, and conduct periodic reviews of PII inventories to ensure the collection and maintenance of the PII is necessary and appropriate, as well as accurate, timely, and complete.

- TR-2, System of Records Notices and Privacy Act Statements, requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

Explain how accuracy of the new data is ensured. Describe the process used for checking accuracy or explain why the system does not check for accuracy. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

This question is related to privacy controls AR-7, Privacy-Enhanced System Design and Development, and DI-1, Data Quality.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems that employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII and to conduct periodic reviews of information systems.

- DI-1, Data Quality, requires organizations to take steps to confirm the accuracy, relevance, timeliness and completeness of PII that is collected or created; collect PII directly from individuals to the greatest extent practicable; check and correct any inaccurate or outdated PII used by programs of information systems; and issue guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. This may include verifying data as it is collected or entered into systems, verifying sources of data if not collected directly from the individual, and reviewing and updating PII holdings regularly to ensure accuracy, relevance, and completeness.

F. Are the data or the processes being consolidated?

If the data is being consolidated, that is, combined or united into one system, application, or process, then the existing controls should remain to protect the data. DOI IT security policies describe technical controls associated with identification and authentication that prevents unauthorized people or processes from accessing data. If needed, strengthen the control(s) to ensure that the data is not inappropriately accessed or used by unauthorized individuals. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources".

This question is related to privacy controls AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

- AR-2, Privacy Impact and Risk Assessment, requires organizations to conduct PIAs and assess privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of PII.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

Describe the process by which an individual receives access to the information within the system. Explain what roles these individuals have and their level of access. If remote access to the system is allowed or external storage or communication devices interact with the

system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication). Do users have "read-only" access or are they authorized to make changes in the system?

Also, consider "other" users who may not be as obvious, such as the Government Accountability Office (GAO) or the Inspector General, database administrators or contractors. Also include those listed in the Privacy Act SORN under the "Routine Uses" section for Privacy Act systems.

This question is related to privacy controls AR-3, Privacy Requirements for Contractors and Service Providers; AR-7, Privacy-Enhanced System Design and Development; and TR-2, System of Records Notices and Privacy Act Statements.

- AR-3, Privacy Requirements for Contractors and Service Providers, requires organizations to establish privacy roles, responsibilities, and access requirements for contractors and service providers, and to include privacy requirements in contracts and other acquisition-related documents.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems that employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII and to conduct periodic reviews of information systems.

- TR-2, System of Records Notices and Privacy Act Statements, , requires organizations to publish SORNs in the *Federal Register* to provide notice to the public on systems of records maintained on individuals; and to provide Privacy Act Statements when collecting PII directly from individuals to provide notice to individuals on the authority for the collection, the purpose and uses of the information collected, and whether providing the information is mandatory or optional, as well as any consequences for not providing the requested information. The Privacy Act allows agencies to claim exemptions from certain provisions of the Privacy Act under special circumstances such as for the protection of criminal law enforcement investigations. In these cases, the SORN that covers the records will indicate if any exemptions are claimed. DOI has promulgated rules to exempt certain systems of records from specific provisions of the Privacy Act, which may include individual notification and access, the requirement to provide an accounting of disclosures to upon request from an individual, providing a Privacy Act Statement at the time of collection, and other provisions. The applicable SORN will include any exemptions claimed and a list of exempt systems may be viewed at 43 CFR 2.254.

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

Users are normally only given access to certain data on a "need-to-know" basis for information that is needed to perform an official function. Care should be given to avoid "open systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system or application. However, access should be restricted when 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 in the authorities section.

DOI IT security policies describe the practice of applying logical access controls, which are system-based means by which the ability is explicitly enabled or restricted. It is the responsibility of Information System Owners to ensure no unauthorized access is occurring.

This question is related to privacy controls AR-3, Privacy Requirements for Contractors and Service Providers; AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

- AR-3, Privacy Requirements for Contractors and Service Providers, requires organizations to establish privacy roles, responsibilities, and access requirements for contractors and service providers, and to include privacy requirements in contracts and other acquisition-related documents.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems that employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII and to conduct periodic reviews of information systems. For example, some of these controls may include access restrictions, audit features, alerts, and encryption.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

If contractors are involved in the development, design or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? When a contract provides for the operation of a system of records on behalf of 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 CFR Part 2: Government Contracts). The Federal Acquisition Regulations (FAR) also require that certain information be included in contract language and certain processes be in place (see FAR at 48 CFR 24.102(a) and DOI Acquisition Regulation (DIAR) at 48 CFR 1424.1).

This question is directly related to privacy control AR-1, Governance and Privacy Program, and AR-3, Privacy Requirements for Contractors and Service Providers.

- AR-1, Governance and Privacy Program, requires organizations to develop and implement policies and procedures that govern privacy and security controls for programs, information systems, or technologies involving PII; demonstrate accountability for the protection of PII; and monitor compliance with privacy controls and privacy operations. This includes oversight of privacy requirements for contracts and service providers.

- AR-3, Privacy Requirements for Contractors and Service Providers, requires organizations to establish privacy roles, responsibilities, and access requirements for contractors and service providers, and to include privacy requirements in contracts and other acquisition-related documents to protect PII.

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

Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.

This question is directly related to privacy controls AR-4, Privacy Monitoring and Auditing, and UL-1, Internal Use.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- UL-1, Internal Use, which requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

Most systems now provide the capability to identify, locate, and monitor individuals (e.g., audit trail systems/applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.

This question is related to privacy controls AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems that employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII and to conduct periodic reviews of information systems.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

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

The DOI IT System 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 A&A process requires a SSP outlining the implementation of the technical controls associated with identification and authentication. Examples of information collected may include username, logon date, failed attempts, files accessed, and user actions.

This question is directly related to privacy controls AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems that employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII and to conduct periodic reviews of information systems.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

M. What controls will be used to prevent unauthorized monitoring?

Certain laws and regulations require monitoring for authorized reasons by authorized employees. Describe the controls in place to ensure that only authorized personnel can monitor use of the system. For example, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to audit logs and least privileges. It is the responsibility of Information System Owners and System Managers to ensure no unauthorized monitoring is occurring.

This question is directly related to privacy controls AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems that employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII and to conduct periodic reviews of information systems.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

N. How will the PII be secured?

Discuss how each privacy risk identified was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions.

Do the audit features include the ability to identify specific records each user can access? Describe the different roles in general terms that have been created to provide access to the project information. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

How is the system audited? For example, does the system perform self-audits, or is the system subject to third-party audits or reviews by the Office of Inspector General or GAO?

Does the IT system have automated tools to indicate when information is inappropriately accessed, retrieved or misused? Describe what privacy training is provided to system users. For example, do system administrators take privacy and security training, or other training specific to the system or program office which includes information handling procedures and sensitivity of information? Explain what controls are in place to ensure that users of the system have completed training relevant to the project. Examples of controls include rules of behavior, encryption, secured facilities, firewalls, etc.

This question is directly related to privacy controls AR-3, Privacy Requirements for Contractors and Service Providers; AR-4, Privacy Monitoring and Auditing; AR-5, Privacy Awareness and Training; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

- AR-3, Privacy Requirements for Contractors and Service Providers, requires organizations to establish privacy roles, responsibilities, and access requirements for contractors and service providers, and to include privacy requirements in contracts and other acquisition-related documents.

- AR-4 requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- AR-5, Privacy Awareness and Training, requires organizations to develop, implement, and update a comprehensive training and awareness strategy to ensure that personnel understand privacy responsibilities and procedures; administer basic privacy training and targeted, role-based privacy training for personnel having

responsibility for PII or for activities that involve PII; and ensure that personnel certify acceptance of responsibilities for privacy requirements. Training methods include: mandatory annual privacy awareness training; targeted, role-based training; internal privacy program websites; manuals, guides, and handbooks; slide presentations; privacy events; posters and brochures; and email messages to all employees and contractors. Organizations may provide privacy training with security training such as the mandatory DOI Federal Information Systems Security Awareness (FISSA)+ Privacy and Records Management training course.

- AR-7, Privacy-Enhanced System Design and Development, requires organizations to design information systems that employ technologies and system capabilities that automate privacy controls on the collection, use, retention, and disclosure of PII and to conduct periodic reviews of information systems.

- UL-1, Internal Use, requires that organizations take steps to ensure that PII is only used for legally authorized purpose(s) and in a manner compatible with the Privacy Act and applicable published system of records notices.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

Although all employees who have access to information in a Privacy Act system have some responsibility for protecting and safeguarding that information, often the Information System Owner and Privacy Act System Manager (identified in the Privacy Act SORN) share the responsibility for protecting the privacy rights of employees and the public. For Privacy Act responsibilities refer to 383 Department Manual Chapters 1-13 and DOI Privacy Act regulations at 43 CFR Part 2. Also, describe how Privacy Act complaints and requests for redress or amendment of records are addressed.

This question is related to privacy controls AR-1, Governance and Privacy Program; AR-4, Privacy Monitoring and Auditing; AR-5, Privacy Awareness and Training; IP-3, Redress; and IP-4, Complaint Management. These controls require organizations to monitor and audit privacy controls and internal privacy policy to promote accountability.

- AR-1, Governance and Privacy Program, requires organizations to develop and implement policies and procedures that govern privacy and security controls for programs, information systems, or technologies involving PII; demonstrate accountability for the protection of PII; and monitor compliance with privacy controls and privacy operations.

- AR-4 requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

- AR-5, Privacy Awareness and Training, requires organizations to develop, implement, and update a comprehensive training and awareness strategy to ensure that personnel understand privacy responsibilities and procedures; administer basic privacy training and targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII; and ensure that personnel certify acceptance of responsibilities for privacy requirements. Training methods include: mandatory annual privacy awareness training; targeted, role-based training; internal privacy program websites; manuals, guides, and handbooks; slide presentations; privacy events; posters and brochures; and email messages to all employees and contractors. Organizations may provide privacy training with security training such as the mandatory DOI Federal Information Systems Security Awareness (FISSA)+ Privacy and Records Management training course.

- IP-3, Redress, requires organizations to provide a process for individuals to correct or amend inaccurate PII maintained by the organization. This facilitates accuracy and demonstrates organizational commitment to data quality, and is especially important in areas where inaccuracy of data may result in negative determinations about individuals or a denial of benefits or services. Such inaccurate data shared through the information sharing environment may also have a negative impact on the privacy, civil rights, and civil liberties of affected individuals. The organization must establish a process for assessing requests for redress, disseminating any corrections or amendments made to the PII maintained and shared with other authorized users of the PII, such as external third parties or partners in the ISE.

- IP-4, Complaint Management, requires organizations to implement a process for receiving and responding to complaints or questions from individuals about privacy practices. The complaint management process or mechanism should be accessible by the public, and include appropriate contact information necessary to submit a complaint, as well as tracking mechanisms to ensure that all complaints received are reviewed and appropriately addressed in a timely manner.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

This may be the Information System Owner and Privacy Act System Manager, or may be another individual with designated responsibility, or otherwise stipulated by contract or in

language contained in an agreement (e.g., Head of the Bureau/Office or Program Manager). There may be multiple responsible officials. Consider a system that contains several databases from different program offices; there may be one information system owner and several Privacy Act system managers. Also, describe who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information. Refer to OMB Circulars A-123, "Management Accountability", and A-130, "Management of Federal Information Resources".

This question is related to privacy controls AR-1, Governance and Privacy Program; AR-3, Privacy Requirements for Contractors and Service Providers; and AR-4, Privacy Monitoring and Auditing, which require organizations to monitor and audit privacy controls and privacy policy to promote accountability.

- AR-1, Governance and Privacy Program, requires organizations to develop and implement policies and procedures that govern privacy and security controls for programs, information systems, or technologies involving PII; demonstrate accountability for the protection of PII; and monitor compliance with privacy controls and privacy operations.

- AR-3, Privacy Requirements for Contractors and Service Providers, requires organizations to establish privacy roles, responsibilities, and access requirements for contractors and service providers, and to include privacy requirements in contracts and other acquisition-related documents to ensure the protection of PII.

- AR-4, Privacy Monitoring and Auditing, requires organizations to monitor and audit privacy controls and internal privacy policy to promote accountability, assess adequacy of privacy protections, address gaps in compliance with privacy requirements, and take corrective actions.

6.5 Review and Approval

All PIAs conducted must contain approving signatures by the following officials to indicate that the official reviewed the PIA and any supporting artifacts to ensure any risks associated with the management of privacy data are identified, evaluated and addressed.

A. Information System Owner. This official has overall responsibility for the operation or maintenance of an information system and compliance with legal and policy requirements.

B. Information System Security Officer. The Chief Information Security Officer may also approve PIAs or Adapted PIAs for third-party websites and social media applications.

C. Privacy Officer. The Departmental Privacy Officer reviews PIAs for Department-wide and Office of the Secretary systems. Bureau/Office Privacy Officer reviews PIA for systems developed, operated or maintained at the bureau or office level.

D. Reviewing Official. The DOI CIO is the SAOP and the Reviewing Official for the Department and must approve all Department-wide PIAs. Bureau/Office ADIRs are Reviewing Officials on PIAs for systems developed, operated or maintained by a bureau or office. In accordance with OMB policy and NIST standards, the agency SAOP must approve the privacy controls implemented for information systems prior to granting an Authority to Operate. This SAOP approval is demonstrated by the PIA review and approval process.

Section 7.0 - DOI Adapted PIA

OMB issued a memorandum on December 29, 2011, to agency CIOs requesting that agencies use the model PIA to develop an adapted PIA that is tailored to assess privacy risks when engaging the public through the use of third-party websites and applications. The DOI Adapted PIA in Appendix B contains general guidance and examples to help prepare quality responses to the questions in the template to facilitate proper assessment of privacy risks associated with agency use of third-party websites and applications. An Adapted PIA must be completed for all official use of third-party websites and applications to ensure the privacy risks are identified and mitigated.

One Adapted PIA may be conducted to cover multiple websites or applications as long as the agency's practices are substantially similar across each website and application. However, any use of a third-party website or application that raises distinct privacy risks requires a completed Adapted PIA specifically for the website or application that includes a tailored analysis of the use of the website or application. Adapted PIAs for Bureau/Office specific use of a third-party website or application may be approved by the Bureau/Office ADIR. Department-wide Adapted PIAs must be elevated to the Departmental Privacy Office for review and approval by the DOI CIO/SAOP. DOI Bureaus and Offices that use third-party websites or create and maintain an official presence on social media applications are responsible for ensuring the use is in accordance with applicable Federal laws, regulations, and DOI privacy, security, and social media policies. DOI has limited control over third-party websites and applications so the assessment and mitigation of privacy risk may be a challenge. It is important that organizations take appropriate steps to assess the inherent risks associated with the use of third-party websites and applications before engaging the public.

Privacy controls are applicable when DOI Bureaus, Offices, or programs collect, use, maintain, or share PII, or otherwise take action that makes PII available, through the use of a third-party website or application. In these cases, the responsible organization must take appropriate steps to identify and assess the privacy risks and implement the appropriate controls and safeguards to mitigate those risks. Identifying and applying privacy controls for agency activities related to the use of third-party websites and applications demonstrates that safeguards were employed to protect the PII that is provided to the agency through program activities that implicate or raise privacy concerns. For example, any agency collection of PII from visitors to a DOI official social media page will require the appropriate authority and a purpose specification for the collection of PII, as well as a Privacy Notice, and the organization must meet any additional requirements under the Privacy Act if the collection of PII results in the creation of a system of records. These requirements are related to privacy controls AP-1, Authority to Collect, AP-2, Purpose Specification, TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements.

Privacy controls may vary dependent on how and why PII is collected, how it is used and shared, where it is maintained and for how long it is maintained, and how it is protected. Program officials should work closely with Bureau/Office Privacy Officers to conduct Adapted PIAs to ensure privacy risks are addressed and privacy requirements are met for all official use of third-party websites and applications.

Section 8.0 - Publishing a PIA

Section 208 of the E-Government Act of 2002 establishes requirements for conducting, reviewing and publishing PIAs for public viewing. PIAs should be clear, unambiguous, and understandable to the general public in order to ensure individuals understand how the government maintains PII.

PIAs demonstrate that the agency has evaluated privacy risks and incorporated protections commensurate with those risks to safeguard the privacy of personal information as agencies implement citizen-centered electronic Government. PIAs promote government transparency by informing the public on the information agencies collect about them and any impact the information collection has on their personal privacy. PIAs also confirm that the information collected is used for the purpose intended; that the information remains timely, relevant, accurate and complete; and that it is protected while agencies have it and that it is maintained only as long as it is needed to fulfill an agency function.

Information System Owners and program managers must work with privacy personnel to determine whether it is appropriate to publish a PIA to the DOI Privacy Impact Assessment website. In accordance with OMB M-03-22, this determination must include an analysis on the sensitivity of the information system as agencies are not required to publish PIAs to the extent

that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information that may be potentially damaging to a national interest, law enforcement effort or competitive business interest. Bureau/Office Privacy Officers should work cooperatively with the program managers and Information System Owners to determine whether PIAs can be published.

Completed Bureau/Office PIAs and Adapted PIAs must be submitted to the Departmental Privacy Office with a request to publish them on the DOI Privacy Impact Assessment website for public viewing. These PIAs must be submitted in the approved PIA formats in accordance with the procedures established by the Departmental Privacy Office. The Departmental Privacy Office will make the final determination on whether to publish a PIA and will manage the inventory of published PIAs on the official DOI Privacy Impact Assessment website. Approved DOI PIAs may only be published to the official DOI Privacy Impact Assessment website. Bureaus and Offices are not authorized to make DOI PIAs publically available on their own websites; however, Bureau and Office web pages may link to the DOI Privacy Impact Assessment website.

Section 9.0 - Privacy Resources

For assistance on conducting Privacy Impact Assessments, please contact your Bureau/Office Privacy Officer. For a list of DOI Privacy Officers, visit http://www.doi.gov/ocio/information_assurance/privacy/privacy-policy-contacts.cfm. Below are links to privacy authorities and resources that may help you in identifying privacy requirements for systems and applying these requirements to your websites, collections of information from individuals, and databases with information on individuals.

The E-Government Act of 2002

- The E-Government Act of 2002: http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
- Federal Information Security Management Act of 2002, 44 U.S.C. §3541, *et seq*: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002: http://www.whitehouse.gov/omb/memoranda/m03-22.html

The Privacy Act, 5 U.S.C. 552a, as amended

- The Privacy Act of 1974, as amended (5 U.S.C. 552a): http://www.justice.gov/opcl/privacy-act-1974
- Office of Management and Budget (OMB) regulations on the Privacy Act. Privacy Act Implementation, Guidelines and Responsibilities, 40 FR 28948 (July 9, 1975): http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf
- OMB Circular A-130, Management of Federal Information Resources. See Appendix I for implementing the Privacy Act and transmittal memorandum: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html
- OMB Privacy Guidance Page: http://www.whitehouse.gov/omb/inforeg_infopoltech#pg
- Department of Justice Privacy Act Overview http://www.justice.gov/opcl/1974privacyact-overview.htm

The Clinger-Cohen Act of 1996

- The Clinger-Cohen Act of 1996, 40 U.S.C. 11101 and 11103: http://uscode.house.gov/view.xhtml?path=/prelim@title40/subtitle3/chapter111&edition=prelim

The Paperwork Reduction Act

- The Paperwork Reduction Act, 44 U.S.C. 35: http://uscode.house.gov/view.xhtml?path=/prelim@title44/chapter35/subchapter1&edition=prelim
- 5 CFR Part 1320.8, Agency collection of information responsibilities: http://www.gpo.gov/fdsys/pkg/CFR-2013-title5-vol3/pdf/CFR-2013-title5-vol3-sec1320-8.pdf

OMB Policy Guidance

- See OMB Privacy Guidance at: http://www.whitehouse.gov/omb/inforeg/infopoltech.html#pg
- OMB M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002: http://www.whitehouse.gov/omb/memoranda/m03-22.html
- OMB M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-19.pdf
- OMB M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information: http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf
- OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-22.pdf
- OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf
- OMB Memo on Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications: http://www.whitehouse.gov/sites/default/files/omb/inforeg/info_policy/model-pia-agency-use-third-party-websites-and-applications.pdf

NIST Guidance

- NIST FIPS Publications: http://csrc.nist.gov/publications/PubsFIPS.html
- NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

- NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
- NIST Special Publications: http://csrc.nist.gov/publications/PubsSPs.html
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII): http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf
- NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Department of the Interior

- DOI Privacy Act regulations at 43 CFR Part 2: http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&rgn=div5&view=text&node=43:1.1.1.1.2&idno=43
- Department Manual privacy chapters can be viewed at 383 DM Ch. 1-13: http://www.doi.gov/ocio/information_assurance/manual.cfm
- DOI Privacy Program Homepage: http://www.doi.gov/ocio/information_assurance/privacy/index.cfm
- DOI Privacy Act system of records notices and Government-wide notices: http://www.doi.gov/ocio/information_assurance/privacy/privacy-act-notices-9-06-06.cfm
- DOI Privacy Portal: https://portal.doi.net/CIO/IAD/ORG/privacy/default.aspx
- Federal Register Document Drafting Handbook (see Ch. 3 on guidelines for Privacy Act System of Records Notices): http://www.archives.gov/federal-register/write/handbook/chapter-3.pdf

Safeguarding and Disposing of Privacy Act Records

- See DOI Manual Section on the Privacy Act at 383 DM 8: http://elips.doi.gov/ELIPS/0/doc/1309/Page1.aspx
- See DOI Records Disposition guidelines at 384 DM 1: http://elips.doi.gov/ELIPS/0/doc/1314/Page1.aspx
- Federal Trade Commission (FTC) Website on Privacy Safeguards: http://www.ftc.gov/privacy/privacyinitiatives/promises_educ.html

Budget Processes and Privacy Requirements

- See privacy requirements for Exhibit 300s at Office of Management and Budget (OMB) Circular A-11, Preparation, Submission and Execution of the Budget, July 26, 2013 (see

Sections 31.8):
http://www.whitehouse.gov/sites/default/files/omb/assets/a11_current_year/a11_2013.pdf

Contracts and Privacy Requirements

- The Privacy Act, Section (m) addresses accountability for Privacy Act systems of records maintained by persons other than agency personnel: http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf
- 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.
    - Federal Acquisition Regulations (FAR) 52.224-1 – Privacy Act Notification
    - 48 CFR 24.103 – Procedures
    - 48 CFR 24.104 – Contract Clauses
    - DOI Acquisition Regulations (DIAR) 1452.224-1, Privacy Act Notification: http://www.ecfr.gov/cgi-bin/text-idx?SID=fe2f1e32019b23b9d7c77d92110e63dc&node=pt48.5.1452&rgn=div5#se48.5.1452_1224_61
- DOI Privacy Act regulations on contracts (43 CFR Part 2.228, Government Contracts): http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=0fc3ab3499768eebc2e3691c8cf88dec&rgn=div5&view=text&node=43:1.1.1.1.2&idno=43#se43.1.2_1228

Interagency Data Sharing

- OMB M-01-05, Guidance on Inter-Agency Sharing of Personal Data – Protecting Personal Privacy, December 20, 2000: http://www.whitehouse.gov/omb/memoranda_m01-05
- Government Accountability Office (GAO) Report of April 2001 (GAO-01-126SP) on Record Linkage and Privacy: http://www.gao.gov/new.items/d01126sp.pdf.

Interior Web Privacy Policy

- The official DOI Privacy Policy: http://www.doi.gov/privacy.cfm
- For websites that collect information from the public a specific notice must address the reason for the information collection, etc. See sample notice at: https://www.volunteer.gov/gov/privacy.cfm
- The official Departmental web disclaimer statement: http://www.doi.gov/disclaimer.cfm

Children's Online Privacy Protection Act Requirements

- DOI Children's Privacy Policy: http://www.doi.gov/privacy_children.cfm.
- For pages directed at Children 13 years or under see the Federal Trade Commission guidance on complying with the Children's Online Privacy Protection Act at: http://www.business.ftc.gov/privacy-and-security/childrens-privacy

National Security Systems Policy

- Committee on National Security Systems Instruction No. 1253, Security Categorization and Control Selection for National Security Systems: https://www.cnss.gov/CNSS/issuances/Instructions.cfm

Glossary

Adapted Privacy Impact Assessment – A document used to assess privacy risks when engaging the public through the use of third-party websites and applications.

Aggregation of Data - Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.

Assessment and Authorization (A&A) - A&A is the process by which the Department assures its information technology systems meet appropriate security and operating standards.

Assistant Director for Information Resources (ADIR) - The official responsible for final approval for Bureau/Office Privacy Impact Assessments. This is the reviewing official who ensures the PIA adequately assesses the privacy and security risks associated with the use of the information system and that remedial action is taken against any privacy deficiencies identified in PIAs.

Authority to Operate – A formal declaration that authorizes operation of a business product and accepts the risk to agency operations.

Authorizing Official - A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Availability - Ensuring timely and reliable access to and use of information.

Chief Information Officer (CIO) - The official responsible for final approval for Department-wide Privacy Impact Assessments. This is the reviewing official who ensures the PIA adequately assesses the privacy and security risks associated with the use of the information system and that remedial action is taken against any privacy deficiencies identified in PIAs.

Chief Information Security Officer (CISO) - The Chief Information Security Officer is responsible for coordinating, developing, and implementing an information security program, and manages the security state of organizational information systems through security authorization processes.

Computer Matching Agreement - An agreement entered into by an organization in connection with a computer matching program to which the organization is a party, as required by the Computer Matching and Privacy Protection Act of 1988. With certain exceptions, a computer

matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records.

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Controlled Unclassified Information - A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

Data Aggregator – A data aggregator is an organization involved in compiling information from detailed databases on individuals and selling that information to others.

Data being consolidated - The process of combining or uniting data into one system, application, or process.

Data Mining - An analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery.

Data Warehouse - A repository of an organization's electronically stored data. Data warehouses are designed to facilitate reporting and analysis. Data warehousing arises in an organization's need for reliable, consolidated, unique and integrated reporting and analysis of its data, at different levels of aggregation.

Derived Data - 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.

DI-3710 Disclosure Accounting Form – Official DOI form used to record the date, nature and purpose of each disclosure from a Privacy Act systems of records, and the name and address of the individual or agency to whom the disclosure is made (See the Privacy Act, 5 U.S.C. 552a (c) for requirements to account for records disclosed to external parties).

Disclosure – A release of information contained in a system of records to any person (other than the person to whom the information pertains), including any employee of the Department of the Interior and employees of other Federal agencies.

Disposition - Actions taken regarding records no longer needed for current government business. For example, (1) transfer to agency storage facilities or Federal records centers, (2) transfer from one Federal agency to another, (3) transfer of permanent records to the National Archives, and (4) disposal of temporary records.

E-Government Act of 2002 – Federal law created to enhance the management and promotion of electronic government services and processes by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to government information and services. Section 208 institutes the requirement for Federal agencies to conduct Privacy Impact Assessments for all electronic systems or collections that contain personally identifiable information on members of the public.

Encryption - The process of encoding electronic information to allow secure transmission of data over the Internet.

Fair Information Practice Principles - Principles that are widely accepted in the United States and internationally as a general framework for privacy and that are reflected in various federal and international laws and policies. In a number of organizations, the principles serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies.

Federal Information Security Management Act of 2002 (FISMA) - The Federal Information Security Management Act was enacted as Title III of the E-Government Act of 2002. It establishes numerous reporting requirements for Federal agencies to measure compliance with various provisions of Federal privacy law, especially addressing electronic records.

Federal Records - Documentary materials created or received in the transaction of government business, regardless of media.

Federal Records Act of 1950 - The Federal Records Act of 1950, as amended, establishes the framework for records management programs in Federal agencies.

Federal Register - The official government daily publication for rules, proposed rules, and notices of Federal agencies and organizations, as well as Executive Orders and other presidential documents. Privacy Act System of Records Notices is published in the *Federal Register*, as are notices associated with Paperwork Reduction Act compliance.

Freedom of Information Act (FOIA) - An Act designed to provide agency records upon request unless certain exemptions apply to all or part of the records. Refer to DOI FOIA regulations for more information about processing information under the FOIA that originated from the Privacy Act System of Records (43 CFR Part 2).

Identification and Authentication - Technical measures used to prevent unauthorized people or processes from accessing data in an information system.

Impact - The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

Individual - A citizen of the United States or an alien lawfully admitted for permanent residence.

Information Collection Clearance Officer (ICCO) - Official responsible for ensuring that all bureau/office information collection activities adhere to the requirements of the Paperwork Reduction Act of 1995 (PRA), Office of Management and Budget directives, and other applicable legislation. The ICCO provides technical assistance, guidance, advice, and training to Information System Owners, Privacy Act System Managers and other bureau/office personnel, and develops bureau/office policies and procedures to ensure compliance with OMB directives and the PRA.

Information in Identifiable Form - Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, SSN 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).

Information Life-Cycle - A process of how information is handled at the collection, use, retention, processing, disclosure and destruction stages.

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner - The official responsible for the overall procurement, development, integration, modification, or operation and maintenance of information systems. The Information System Owner is also responsible for completing the privacy impact assessment, and implementing the legal information resources management requirements such as Privacy, Security, Records Management, Freedom of Information Act, and data administration.

Information System Security Officer (ISSO) – Official appointed by an Information System Owner to ensure implementation of system-level security controls and to maintain system documentation. The ISSO also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system, and must have the detailed knowledge and expertise required to manage the daily security aspects of an information system.

Information Technology (IT) - As defined in the Clinger-Cohen Act, 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.

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Make PII Available - The term "make PII available" includes any agency action that causes PII to become available or accessible to the agency, whether or not the agency solicits or collects it. In general, an individual can make PII available to an agency when he or she provides, submits, communicates, links, posts, or associates PII while using a website or application. "Associate" can include activities commonly referred to as "friend-ing," "following," "liking," joining a "group," becoming a "fan," and comparable functions.

Metadata - Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).

National Security Systems - As defined in the Clinger-Cohen Act, an information system operated by the Federal government, the function, operation or use of which involves:(a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.

Paperwork Reduction Act of 1995 - The Paperwork Reduction Act of 1995 establishes requirements for collecting the same information from ten (10) or more persons, which does not

include Federal employees acting in their official capacity. If you are collecting information from members of the public, you must ensure that you have OMB approval to do so. You should contact your Bureau/Office Information Collection Clearance Officer to determine whether you need to obtain an OMB approval to collect the information.

Person – Under the Paperwork Reduction Act, anyone who is burdened by having to respond to a Federal request for information, except for Federal employees who are responding within the scope of their Federal employment.

Personally Identifiable Information (PII) - Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Privacy Act of 1974 - The Privacy Act (5 U.S.C. 552a) established controls over what personal information the Federal government collects and how it uses or discloses that information. The Privacy Act has four basic objectives: (1) To restrict disclosure of personally identifiable records maintained by agencies; (2) To grant individuals increased rights of access to agency records maintained on them; (3) To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete; and (4) To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Privacy Act Exemption - The Privacy Act authorizes a Federal agency to exempt records or information in a system of records from some of the Privacy Act requirements, if the agency determines that the exemption is necessary.

Privacy Officer - Official responsible for managing and overseeing privacy activities to ensure compliance with Federal privacy laws and policies. The Privacy Officer implements privacy policy, provides guidance, evaluates bureau/office programs, systems and initiatives for potential privacy implications and provides strategies to mitigate or reduce privacy risk.

Privacy Act Statement – When personally identifiable information is collected directly from an individual, that individual must be provided with a Privacy Act Statement that describes the information collection's purpose, planned routine uses, the legal authority for the collection, whether providing the information is voluntary or mandatory, and any consequences for not providing the requested information. It can be included on the form (paper or web-based), in a separate handout, or read to the individual.

Privacy Act System Manager - Official responsible for management of a Privacy Act system of records. The Privacy Act System Manager is usually identified in the published system of records notice; however, this duty may be further delegated to personnel within the agency, bureau or program office. For Privacy Act System Manager responsibilities identified by the Privacy Act, refer to the Departmental Manual Privacy Act Sections, 383 DM 1-13, and DOI Privacy Act regulations at 43 CFR Part 2.

Privacy Act Warning Notice – A notice (paper or electronic) that informs users of the system of records of the restrictions and the penalties for not abiding by those restrictions (See DOI Privacy Act Warning Notice, 383 DM 8, Illustration 1). These notices must be posted on file folders, cabinets, or other storage devices containing privacy files.

Privacy Controls – A set of controls based on international standards and best practices to assist agencies in enforcing privacy requirements derived from Federal legislation, directives, policies, regulations, and standards. NIST SP 800-53 Revision 4, Appendix J, describes the eight privacy control families. The privacy controls are implemented with the PIA to ensure DOI analyzes the privacy risk of an information system.

Privacy Impact Assessment (PIA) - An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Incident - The potential loss of control, compromise, unauthorized disclosure or unauthorized access to PII, whether physical or electronic, and includes both suspected and confirmed incidents (also referred to as a "breach").

Privacy Information - Any information linked, or linkable, to a named individual, whether directly named or indirectly inferred. Such information includes the individual's full name, Social Security number, home address, home telephone number, finger and voice prints, birth date, medical, financial and family information, beliefs and affiliations, and any other information that is identifiable to the individual

Privacy Notice - A brief description that informs individuals on what information is collected and how it will be used by the agency. Because the Privacy Notice should serve to notify individuals before they engage with an agency, a Privacy Notice should be provided on the specific webpage or application where individuals have the opportunity to make PII available to the agency.

Privacy Policy - A single, centrally located statement that is accessible from an agency's official homepage. The Privacy Policy should be a consolidated explanation of the agency's general privacy-related practices that pertain to its official website and its other online activities.

Records Officer - Official responsible for collaborating with the Information System Owner and Privacy Act System Manager to identify or develop records retention schedules with approval by the National Archives and Records Administration for Federal records maintained within the system. The Bureau/Office Records Officer provides guidance to the Information System Owner on the management of records, the appropriate records retention and destruction schedules, and approved disposition methods.

Records Retention Schedule - A list of all records maintained by the agency and how long they need to be kept. Some of the records need to be retained permanently, while others can be destroyed once they have exceeded the minimum retention period. The records retention schedule is a legal authorization to destroy records.

Reviewing Official - The agency official responsible for reviewing and providing final approval on privacy impact assessments. The DOI CIO is the Reviewing Official for the Department and must approve all Department-wide PIAs. Bureau/Office ADIRs are Reviewing Officials for bureau/office specific PIAs. The Reviewing Official ensures that the PIA adequately assesses the privacy and security risks associated with the use of the information system and that remedial action is taken against any privacy deficiencies identified in PIAs.

Routine Use - A use of a record which is compatible with the purpose for which it was collected (these are identified in the Privacy Act system of records notice published in the *Federal Register*). It is important that agency employees comply with the limits of the routine uses listed in the SORN.

Safeguards - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Senior Agency Official for Privacy (SAOP) – The agency official responsible for implementing the privacy provisions of the Privacy Act of 1974, the E-Government Act of 2002, and related privacy laws and policies. The DOI SAOP must approve the Authority to Operate to ensure the privacy controls for a system are implemented.

Sensitive Information - Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that

has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Spatial Data - Data that describes the attributes of some object or thing occurring at one or more locations or in a region in geographic space.

System of Records – A 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.

System of Records Notice (SORN) - A Privacy Act notice that is published in the *Federal Register* for all collections of information on individuals where the information is retrieved by a name or other personal identifier.

Third-party websites or applications - Web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a ".com" website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency's official website.

Acronyms

A&A	Assessment and Authorization
ADIR	Assistant Director for Information Resources
ATO	Authority to Operate
BCISO	Bureau/Office Chief Information Security Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment and Management
DIAR	DOI Acquisition Regulation
DOI	Department of the Interior
DM	Departmental Manual
EFS	Enterprise Forms System
FAR	Federal Acquisition Regulations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FISSA	Federal Information Systems Security Awareness
FOIA	Freedom of Information Act
GAO	Government Accountability Office
GSS	General Support System
ICCO	Information Collection Clearance Officer
ICR	Information Collection Request
ISE	Information Sharing Environment
ISSO	Information System Security Officer
IT	Information Technology
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
PRA	Paperwork Reduction Act
SAOP	Senior Agency Official for Privacy
SORN	System of Records Notice
SP	Special Publication
SSN	Social Security Number
SSP	System Security Plan

Appendix A: DI-4001 PIA Form

DI-4001 09/2014
U.S. Department of the Interior

U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs 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. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project	Date
Appendix A - Sample DI-4001 PIA Form	09/30/2014

Bureau/Office	Bureau/Office Contact Title
Office of the Secretary	Privacy Officer

Point of Contact Email	First Name	M.I.	Last Name	Phone
Privacy Officer@ios.doi.gov	Privacy		Officer	(202) 208-0000

Address Line 1
1849 C St NW

Address Line 2
Mail Stop MIB

City	State/Territory	Zip
Washington	District of Columbia	20240

Section 1. General System Information

A. Is a PIA required?

Yes

Yes, information is collected from or maintained on

Federal personnel and/or Federal contractors

B. What is the purpose of the system?

Describe the purpose of the system and how it relates to the program office's and Department's mission. Include the context and background necessary to understand the purpose, the name of the program office and the technology, project or collection being assessed.

This question is directly related to privacy control AP-2, Purpose Specification.

Page 1 of 13

C. What is the legal authority?

A Federal law, Executive Order of the President (EO), or DOI requirement must authorize the collection and maintenance of a system of records. For Privacy Act systems, the response should reflect the information provided in the authority section of the Privacy Act system of records notice.

This question is directly related to privacy controls AP-1, Authority to Collect; and UL-1, Internal Use.

D. Why is this PIA being completed or modified?

Other

Describe

Indicate why the PIA is being conducted. For example, the system is being significantly modified or two systems are being merged together.

This question is related to privacy controls AP-2, Purpose Specification; and AR-7, Privacy-Enhanced System Design and Development.

E. Is this information system registered in CSAM?

Yes

System Security Plan (SSP) Name

Test System

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

Subsystem Name	Purpose	Contains PII	Describe
Subsystem A	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.	Yes	This question is related to privacy controls AR-1, Governance and Privacy Program, and AR-4, Privacy Monitoring and Auditing.

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

Yes

List Privacy Act SORN Identifier(s)

A Privacy Act SORN is required if the information system or electronic collection contains information about individuals that is retrieved by name or other unique identifier. Provide the DOI or Government-wide Privacy Act SORN identifier and ensure it is entered in CSAM for this system. For new SORNS being developed, select "Yes" and provide a detailed explanation. Contact your Bureau Privacy Officer for assistance identifying the appropriate Privacy Act SORN (s).

This question is directly related to privacy control TR-2, System of Records Notices and Privacy Act Statements.

H. Does this information system or electronic collection require an OMB Control Number?

Yes

Describe

The Paperwork Reduction Act requires an OMB Control Number for certain collections of information from ten or more members of the public. If information is collected from members of the public, contact your Bureau Information Collection Clearance Officer for assistance to determine whether you need to obtain OMB approval. Please include all OMB Control Numbers and Expiration Dates that are applicable.

This question is related to privacy controls AR-2, Privacy Impact and Risk Assessment; and DI-1, Data Quality.

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☐ Name	☐ Religious Preference	☐ Social Security Number (SSN)
☐ Citizenship	☐ Security Clearance	☐ Personal Cell Telephone Number
☐ Gender	☐ Spouse Information	☐ Tribal or Other ID Number
☐ Birth Date	☐ Financial Information	☐ Personal Email Address
☐ Group Affiliation	☐ Medical Information	☐ Mother's Maiden Name
☐ Marital Status	☐ Disability Information	☐ Home Telephone Number
☐ Biometrics	☐ Credit Card Number	☐ Child or Dependent Information
☐ Other Names Used	☐ Law Enforcement	☐ Employment Information
☐ Truncated SSN	☐ Education Information	☐ Military Status/Service
☐ Legal Status	☐ Emergency Contact	☐ Mailing/Home Address
☐ Place of Birth	☐ Driver's License	
☒ Other	☐ Race/Ethnicity	

Specify the PII collected.

Identify all the categories of PII that will be collected, stored, used, maintained or disseminated. Describe any additional categories of PII not already indicated, as well as any new information that is created (for example, an analysis or report), and describe how this is done and the purpose of that information.

This question is related to privacy control SE-1, Inventory of Personally Identifiable Information.

B. What is the source for the PII collected? Indicate all that apply.

☐ Individual	☐ Tribal agency	☐ DOI records	☐ State agency
☐ Federal agency	☐ Local agency	☐ Third party source	☒ Other

Describe

Include all sources of PII collected. For example, information may be collected directly from an individual through a written form, website collection, or through interviews over the phone or in person. Information may also come from agency officials and employees, agency records, from a computer readable extract from another system, or may be created within the system itself. If information is being collected through an interface with other systems, commercial data aggregators, or other agencies, list the source(s) and explain why information from sources other than the individual is required.

This question is related to privacy controls DI-1, Data Quality; IP-1, Consent; TR-1, Privacy Notice; and TR-2, System of Records Notices and Privacy Act Statements.

C. How will the information be collected? Indicate all that apply.

☐ Paper Format	☐ Face-to-Face Contact	☐ Fax	☐ Telephone Interview
☐ Email	☐ Web Site	☒ Other	☐ Information Shared Between Systems

Describe

Indicate all the formats or methods for collecting PII that will be used. If the system receives information from another system, such as a transfer of financial information or response to a background check, describe the system from which the information originates, how the information is used, and how the systems interface.

This question is related to privacy controls AR-7, Privacy-Enhanced System Design and Development; DI-1, Data Quality; TR-1, Privacy Notice; TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

D. What is the intended use of the PII collected?

Describe the intended uses of the PII collected and maintained in the system and provide a detailed explanation on how the data will be used. The intended uses must be relevant to the purpose of the system; for Privacy Act systems, uses must be consistent with the published system of records notice.

This question is related to privacy controls AP-2, Purpose Specification; TR-1, Privacy Notice; TR-2, System of Records Notices and Privacy Act Statements; UL-1, Internal Use; and UL-2, Information Sharing with Third Parties.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office

Describe the bureau or office and how the data will be used.

Indicate all the parties, both internal and external to DOI, with whom PII will be shared. Identify other DOI offices with assigned roles and responsibilities within the system, or with whom information is shared, and describe how and why information is shared. Also, identify other federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared; and describe any routine information sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. If sharing is pursuant to a Computer Matching Agreement, provide an explanation. For Privacy Act systems, describe how an accounting for the disclosure is maintained.

This question is related to privacy controls AR-3, Privacy Requirements for Contractors and Service Providers; AR-8, Accounting of Disclosures; DI-2, Data Integrity and Data Integrity Board; TR-1, Privacy Notice; TR-2, System of Records Notices and Privacy Act Statements; UL-1, Internal Use; and UL-2, Information Sharing with Third Parties.

☒ Other Bureaus/Offices

Describe the bureau or office and how the data will be used.

See above.

☒ Other Federal Agencies

Describe the federal agency and how the data will be used.

See above.

☒ Tribal, State or Local Agencies

Describe the Tribal, state or local agencies and how the data will be used.

See above.

☒ Contractor

Describe the contractor and how the data will be used.

See above.

☒ Other Third Party Sources

Describe the third party source and how the data will be used.

See above.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

Yes

Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.

If "Yes," describe the method by which individuals can decline to provide information or how individuals consent to specific uses. If "No," state the reason why individuals cannot object or why individuals cannot give or withhold their consent.

This question is directly related to privacy control IP-1, Consent.

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☐ Privacy Act Statement ☐ Privacy Notice ☒ Other ☐ None

Describe each applicable format.

Describe how notice is provided to the individual about the information collected, the right to consent to uses of the information, and the right to decline to provide information. For example, privacy notice to individuals may include Privacy Act Statements, posted Privacy Notices, privacy policy, and published SORNs and PIAs. Describe each format used and, if possible, provide a copy of the Privacy Act Statement, Privacy Notice, or a link to the applicable privacy policy, procedure, PIA or referenced SORN Federal Register citation (e.g., XX FR XXXX, Date) for review. Also describe any Privacy Act exemptions that may apply and reference the Final Rule published in the Code of Federal Regulations (43 CFR Part 2).

This question is directly related to privacy controls TR-1, Privacy Notice; and TR-2, System of Records Notices and Privacy Act Statements.

H. How will data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Describe how data is retrieved from the system. For example, is data retrieved manually or via reports generated automatically? Are specific retrieval identifiers used or does the system use key word searches? Be sure to list the identifiers that will be used to retrieve data (e.g., name, case number, Tribal Identification Number, subject matter, date, etc.).

This question is related to privacy controls TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

I. Will reports be produced on individuals?

Yes

What will be the use of these reports? Who will have access to them?

Indicate whether reports will be produced on individuals. Provide an explanation on the purpose of the reports generated, how the reports will be used, what data will be included in the reports, who the reports will be shared with, and who will have access to the reports. Many systems have features that allow reports to be generated on data in the system or on user actions within the system.

This question is related to privacy controls AR-4, Privacy Monitoring and Auditing; and UL-1, Internal Use.

Section 3. Attributes of System Data

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

Data accuracy and reliability are important requirements in implementing the Privacy Act which requires that agencies only maintain data that is accurate, relevant, timely, and complete about individuals. 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.

This question is related to privacy controls DI-1, Data Quality; DM-1, Minimization of Personally Identifiable Information; and IP-3, Redress.

B. How will data be checked for completeness?

Describe the procedures to ensure data is checked for completeness. To the extent practical, PII should be checked for completeness to ensure accuracy within the context of the use of the data.

This question is related to DI-1, Data Quality.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Describe the steps or procedures taken to ensure the data is current and not out-of-date. Where are they documented? For example, are they outlined in standard operating procedures or data models? Data that is not current also affects the relevancy and accuracy of the data. This is particularly true with data warehousing. A data warehouse is a repository of an organization's electronically stored data and is designed to facilitate reporting and analysis. A data warehouse may contain data that is not current which would cause a domino effect throughout the data stores.

This question is related to DI-1, Data Quality.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

Identify all applicable records retention schedules or explain at what development stage the proposed records retention schedule is in. Information system owners must consult with Bureau/Office Records Officers early in the development process to ensure that appropriate retention and destruction schedules are identified, or to develop a records retention schedule for the records contained in the information system. Be sure to include applicable records retention schedules for different types of information or subsets of information and describe if subsets of information are deleted and how they are deleted.

This question is directly related to privacy control DM-2, Data Retention and Disposal.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Describe policies and procedures for how PII that is no longer relevant and necessary is purged. This may be obtained from records retention schedules, the Departmental Manual, bureau/office records management policies, or standard operating procedures.

This question is directly related to privacy control DM-2, Data Retention and Disposal.

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

Describe and analyze the major potential privacy risks identified and discuss the overall impact on the privacy of employees or individuals. Include a description of how the program office has taken steps to protect individual privacy and mitigate the privacy risks. Provide an example of how information is handled at each stage of the information life cycle. Also discuss privacy risks associated with the sharing of information outside of the Department and how those risks were mitigated. Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department.

This question is related to privacy controls AR-2, Privacy Impact and Risk Assessment; AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; DM-1, Minimization of Personally Identifiable Information; DM-2, Data Retention and Disposal; DM-3, Minimization of PII Used in Testing, Training, and Research; SE-1, Inventory of Personally Identifiable Information; UL-1, Internal Use, and UL-2, Information Sharing with Third Parties.

Section 4. PIA Risk Review

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

Yes

Explanation

Describe how the use of the system or information collection relates to the purpose of the underlying mission of the organization. Is the information directly relevant and necessary to accomplish the specific purposes of the system? For Privacy Act systems, the Privacy Act at 5 U.S.C. 552a(e)(1) requires that each agency shall maintain in its records only such information about an individual that is relevant and necessary to accomplish an agency purpose required by statute or by executive order of the President.

This question is related to privacy controls AP-2, Purpose Specification; DM-1, Minimization of Personally Identifiable Information; TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

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

Yes

Explain what risks are introduced by this data aggregation and how these risks will be mitigated.

Does the technology create new data or conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? Is data aggregated in a way that will permit system users to easily draw new conclusions or inferences about an individual? Electronic systems can sift through large amounts of information in response to user inquiry or programmed functions, or perform complex analytical tasks resulting in other types of data, matching, relational or pattern analysis, or reporting. Discuss the results generated by these uses and include an explanation on how the results are generated, whether by the information system or manually by authorized personnel. Explain the purpose and what will be done with the newly derived data. Derived data is obtained from a source for one purpose and then used to deduce/infer a separate and distinct bit of information to form additional information that is usually different from the original source information. Aggregation of data is the taking of various data elements and turning it into a composite of all the data to form another type of data, e.g., tables or data arrays.

This question is related to privacy controls AP-2, Purpose Specification; AR-2, Privacy Impact and Risk Assessment; and UL-1, Internal Use.

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

Yes

Explanation

Will the results or new data be placed in individuals' records? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

This question is related to privacy controls AP-2, Purpose Specification; AR-2, Privacy Impact and Risk Assessment; DI-1, Data Quality; DM-1, Minimization of Personally Identifiable Information; TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

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

Yes

Explanation

Will the new data be used to make determinations about individuals or will it have any other effect on the subject individuals? Explain in detail the purpose of creating the new data, how it will be used, by whom it will be used, with whom it will be shared, and any resulting effect on individuals.

This question is related to privacy controls AP-2, Purpose Specification; AR-2, Privacy Impact and Risk Assessment; DI-1, Data Quality; DM-1, Minimization of Personally Identifiable Information; TR-2, System of Records Notices and Privacy Act Statements; and UL-1, Internal Use.

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

Explain how accuracy of the new data is ensured. Describe the process used for checking accuracy. Also explain why the system does not check for accuracy. Describe any technical solutions, policies, or procedures focused on improving data accuracy and integrity of the project.

This question is related to privacy controls AR-7, Privacy-Enhanced System Design and Development; and DI-1, Data Quality.

F. Are the data or the processes being consolidated?

Yes, data is being consolidated

Describe the controls that 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 should remain to protect the data. If needed, strengthen the control(s) to ensure that the data is not inappropriately accessed or used by unauthorized individuals. Minimum sets of controls are outlined in OMB Circular A-130, Appendix III. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of identification and authentication that is a technical measure that prevents unauthorized people or processes from accessing data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication.

This question is related to privacy controls AR-2, Privacy Impact and Risk Assessment; and UL-1, Internal Use.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☐ Users ☐ Developers ☐ System Administrator

☐ Contractors ☒ Other

Describe

Describe the process by which an individual receives access to the information within the system. Explain what roles these individuals have and their level of access. If remote access to the system is allowed or external storage or communication devices interact with the system, describe any measures in place to secure the transmission and storage of data (e.g., encryption and/or two-factor authentication). Do users have "read-only" access or are they authorized to make changes in the system? Also consider "other" users who may not be as obvious, such as the GAO or the Inspector General, database administrators, website administrators or system administrators. Also include those listed in the Privacy Act system of records notice under the "Routine Uses" section when a Privacy Act system of records notice is required.

This question is related to privacy controls AR-3, Privacy Requirements for Contractors and Service Providers; AR-7, Privacy-Enhanced System Design and Development; and TR-2, System of Records Notices and Privacy Act Statements.

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

Users are normally only given access to certain data on a "need-to-know" basis for information that is needed to perform an official function. Care should be given to avoid "open systems" where all information can be viewed by all users. System administrators may be afforded access to all of the data depending upon the system or application. However, access should be restricted when users may not need to have access to all the data. For more guidance on this, refer to the Federal Information Processing Standards (FIPS) Publications in the authorities section. The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) describe the practice of applying logical access controls, which are system-based means by which the ability is explicitly enabled or restricted. It is the responsibility of information system owners to ensure no unauthorized access is occurring.

This question is related to privacy controls AR-3, Privacy Requirements for Contractors and Service Providers; AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

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

Yes

Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?

If contractors are involved in the development, design or maintenance of the system, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? When a contract provides for the operation of a system of records 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 CFR Part 2). The Federal Acquisition Regulations also require that certain information be included in contract language and certain processes must be in place (see FAR 48 CFR 24.102(a) and DOI Acquisition Regulation at 48 CFR 1424.1).

This question is directly related to privacy control AR-1, Governance and Privacy Program; and AR-3, Privacy Requirements for Contractors and Service Providers.

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

Yes

Explanation

Are there new technologies used to monitor activities of the individual in any way? Access logs may already be used to track the actions of users of a system. Describe any new software being used, such as keystroke monitoring.

This question is directly related to privacy controls AR-4, Privacy Monitoring and Auditing; and UL-1, Internal Use.

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

Yes

Explanation

Most systems now provide the capability to identify and monitor individual's actions in a system (e.g., audit trail systems/ applications). For example, audit logs may record username, time and date of logon, files accessed, or other user actions. Check system security procedures for information to respond to this question.

This question is related to privacy controls AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

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

The DOI Security Control Standards (based on NIST SP 800-53 and FedRAMP) detail how audit logs should be used for DOI systems. Provide what audit activities are maintained to record system and user activity including invalid logon attempts and access to data. The IT Security A&A process requires a system security plan outlining the implementation of the technical controls associated with identification and authentication of users to the system. Examples of information collected may include username, logon date, number of failed logon attempts, files accessed, and other user actions on the system.

This question is directly related to privacy controls AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

M. What controls will be used to prevent unauthorized monitoring?

Certain laws and regulations require monitoring for authorized reasons by authorized employees. Describe the controls in place to ensure that only authorized personnel can monitor use of the system. For example, business rules, internal instructions, posting Privacy Act Warning Notices address access controls, in addition to audit logs and least privileges. It is the responsibility of information system owners and system managers to ensure no unauthorized monitoring is occurring.

This question is directly related to privacy controls AR-4, Privacy Monitoring and Auditing; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☐ Security Guards	☐ Secured Facility	☐ Identification Badges	☐ Combination Locks
☐ Key Cards	☐ Closed Circuit Television	☐ Safes	☐ Locked Offices
☐ Locked File Cabinets	☐ Cipher Locks	☒ Other	

Describe

Discuss how each privacy risk identified was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions. Do the audit features include the ability to identify specific records each user can access? How is the system audited? For example, does the system perform self audits, or is the system subject to third party audits or reviews by the Office of Inspector General or Government Accountability Office (GAO). Does the IT system have automated tools to indicate when information is inappropriately accessed, retrieved or misused? Describe what privacy and security training is provided to system users. Examples of controls include rules of behavior, encryption, secured facilities, firewalls, etc.

This question is directly related to privacy controls AR-3, Privacy Requirements for Contractors and Service Providers; AR-4, Privacy Monitoring and Auditing; AR-5, Privacy Awareness and Training; AR-7, Privacy-Enhanced System Design and Development; and UL-1, Internal Use.

(2) Technical Controls. Indicate all that apply.

☐ Password	☐ Intrusion Detection System (IDS)
☐ Firewall	☐ Virtual Private Network (VPN)
☐ Encryption	☐ Public Key Infrastructure (PKI) Certificates
☐ User Identification	☐ Personal Identity Verification (PIV) Card
☐ Biometrics	
☒ Other	

Describe

See above.

(3) Administrative Controls. Indicate all that apply.

☐ Periodic Security Audits	☐ Regular Monitoring of Users' Security Practices
☐ Backups Secured Off-site	☐ Methods to Ensure Only Authorized Personnel Have Access to PII
☐ Rules of Behavior	☐ Encryption of Backups Containing Sensitive Data
☐ Role-Based Training	☐ Mandatory Security, Privacy and Records Management Training
☒ Other	

Describe

See above.

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

Although all employees who have access to information in a Privacy Act system have responsibility for protecting and safeguarding that information, often the information system owner and Privacy Act system manager share the responsibility for protecting the privacy rights of employees and the public. For Privacy Act responsibilities refer to 383 Department Manual Chapters 1-13 and DOI Privacy Act regulations at 43 CFR Part 2. Also, describe how Privacy Act complaints and requests for redress or amendment of records are addressed.

This question is related to privacy controls AR-1, Governance and Privacy Program; AR-4, Privacy Monitoring and Auditing; AR-5, Privacy Awareness and Training; IP-3, Redress; and IP-4, Complaint Management.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

This may be the information system owner and Privacy Act system manager, or may be another individual with designated responsibility, or otherwise stipulated by contract or in language contained in an agreement (e.g., Head of the Bureau or Program Manager). There may be multiple responsible officials. Consider a system that contains several databases from different program offices; there may be one information system owner and several Privacy Act system managers. Also, describe who is responsible for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information.

This question is related to privacy controls AR-1, Governance and Privacy Program; AR-3, Privacy Requirements for Contractors and Service Providers; and AR-4, Privacy Monitoring and Auditing.

Section 5. Review and Approval

Information System Owner

Email: System_Owner@ios.doi.gov

First Name	M.I.	Last Name	Title
System		Owner	Program Manager

Bureau/Agency	Phone	Date
Office of the Secretary	(202) 208-1000	09/29/2014

Electronically signed by: System Owner
Date: undefined
Reference number: DI-4001-c7c4a37eVK
U.S. Department of the Interior | Enterprise Forms System

Information System Security Officer

Email: Security_Officer@ios.doi.gov

First Name	M.I.	Last Name	Title
Security		Officer	Information System Security Officer

Bureau/Agency	Phone	Date
Office of the Secretary	(202) 208-1001	09/29/2014

Electronically signed by:Security Officer
Date: Tue Sep 30 2014 15:54:07 GMT-0400
Reference number: DI-4001-c7c4a37eVK
U.S. Department of the Interior | Enterprise Forms System

Privacy Officer

Email: Privacy_Officer@ios.doi.gov

First Name	M.I.	Last Name	Title
Privacy		Officer	Privacy Officer

Bureau/Agency	Phone	Date
Office of the Secretary	(202) 208-1002	09/29/2014

Electronically signed by: Privacy Officer
Date: Tue Sep 30 2014 16:01:12 GMT-0400
Reference number: DI-4001-c7c4a37eVK
U.S. Department of the Interior | Enterprise Forms System

Reviewing Official

Email: Reviewing_Official@ios.doi.gov

First Name	M.I.	Last Name	Title
Reviewing		Official	Reviewing Official

Bureau/Agency	Phone	Date
Office of the Secretary	(202) 208-1003	09/29/2014

Electronically signed by: Reviewing Official
Date: Tue Sep 30 2014 16:20:04 GMT-0400
Reference number: DI-4001-c7c4a37eVK
U.S. Department of the Interior | Enterprise Forms System

Page 13 of 13

Appendix B: Adapted Privacy Impact Assessment

Adapted Privacy Impact Assessment

[Name of Third-Party Website or Application]

[Date]

Contact

[Bureau/Office] Privacy Officer
U.S. Department of the Interior
[address]
[phone number]
[email]

One Privacy Impact Assessment (PIA) may be prepared to cover multiple websites or applications that are functionally comparable as long as agency or bureau practices are substantially similar across each website or application. However, any use of a third-party website or application that raises distinct privacy risks requires a completed Adapted PIA exclusive to the specific website or application. Department-wide PIAs must be elevated to the Office of the Chief Information Officer (OCIO) for review and approval.

SECTION 1: Specific Purpose of the Agency's Use of the Third-Party Website or Application

1.1 What is the specific purpose of the agency's use of the third-party website or application and how does that use fit with the agency's broader mission?

Use plain language to explain the purpose(s) of DOI's use of third-party websites or applications. Provide enough detail to allow the reader to gain a full understanding of the purpose of the use in alignment with DOI's mission. For example, this may include: to facilitate communication, obtain feedback from the public, to provide information about DOI programs, or to provide a service or improve customer service.

1.2 Is the agency's use of the third-party website or application consistent with all applicable laws, regulations, and policies? What are the legal authorities that authorize the use of the third-party website or application?

The President's memorandum on *Transparency and Open Government* and the OMB Director's *Open Government Directive* call on Federal departments and agencies to harness new technologies to engage with the public. These documents may serve as the primary policies underlying the agency's efforts to use the third-party websites or applications. However, the use of third-party websites and applications must comply with all applicable laws, regulations, and policies, in particular those pertaining to privacy, accessibility, information security, and records management. Identify the laws, regulations, and Executive Orders that authorize maintenance of the system or information collection to meet an official program mission or goal. Explain how the authority permits collection and use of the information.

SECTION 2: Any PII that is Likely to Become Available to the Agency Through the Use of the Third-Party Website or Application

2.1 What PII will be made available to the agency?

Describe the types of PII that will become available to DOI. For example, third-party websites or applications may request personally identifiable information (PII) from users during registration, or users can voluntarily provide PII during interactions on the third-party website. For example, users

can provide such information as individual interests, birthday, religious and political views, family members and relationship status, education, occupation and employment, photographs, contact information, and hometown.

Individuals can also make PII available when communicating, submitting, posting, blogging, linking, "friend-ing," "following," "liking," joining a "group," becoming a "fan," and comparable functions. PII may be transmitted through the system during the sign-up/log-on transaction or during subsequent interactions. It is also important to recognize that these activities may make information about a user more widely available than is immediately obvious to the user. For example, a user may post information on one third-party website that may be linked to a different third-party website without the user's knowledge or consent. Note that if PII is posted in a public area or sent to the agency in connection with the transaction of public business, it may become a Federal record.

Users may also transmit PII through the system by commenting on images or videos, or otherwise submitting information. Be sure to make clear whether DOI will have access to this information and how users can take steps to limit DOI's access to PII.

2.2 What are the sources of the PII?

Generally, sources of PII are the users of the third-party website or application, including registered users and visitors who may be commenting or posting. Users may be required to submit PII to the third-party websites or applications at the time of registration. This information is collected and maintained by the third-party websites or applications, but may also be available to DOI. It is important to recognize that DOI may gain access to information in ways that are not immediately obvious to users. Be sure to include all sources of PII, including other Federal agencies, state, local or tribal entities, as well as private organizations.

2.3 Will the PII be collected and maintained by the agency?

This is important as any PII collected and maintained by DOI must be protected and managed in accordance with applicable laws, regulations and policies. Describe any PII collected and maintained, the purpose for the collection, and any controls in place to protect the PII.

2.4 Do the agency's activities trigger the Paperwork Reduction Act (PRA) and, if so, how will the agency comply with the statute?

Consult your Bureau/Office Information Collection Clearance Officer for each use of a third-party website or application. Refer to the April 7, 2010, OMB memorandum entitled, *Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act* to determine whether the Paperwork Reduction Act (PRA) of 1995 will apply. The PRA establishes requirements for collecting the same information from 10 or more persons – this does not include Federal

employees acting in their official capacity. If the PRA does apply, provide OMB Control number(s) for the collection.

SECTION 3: The Agency's Intended or Expected Use of the PII

3.1 Generally, how will the agency use the PII described in Section 2.0?

Describe how the PII will be used and address the potential uses of any PII that is likely to become available. This will provide the public with notice of any future uses or actions, and will identify and address the full range of privacy risks. Also provide alternative approaches that might help to mitigate these risks, such as the option to use an official agency website in lieu of a third-party website. If the Privacy Act applies to the data, the use of the PII must be consistent with the "routine uses" published in the applicable Privacy Act system of records notice.

3.2 Provide specific examples of the types of uses to which PII may be subject.

Describe specific uses for the PII. For example, surveys, contests, or message boards that provide a forum for the public to comment on the agency's activities; recruitment or employee outreach to attract new hires or to inform or receive feedback from current employees; to facilitate access to programs or systems or feedback on those programs. Consider whether this will result in the PII being combined, matched, or otherwise used with PII that is already maintained by the agency on individuals.

SECTION 4: Sharing or Disclosure of PII

4.1 With what entities or persons inside or outside the agency will the PII be shared, and for what purpose will the PII be disclosed?

Describe all the entities to which any PII may be disclosed and the purpose of such disclosure. This may include other Federal, state and local government agencies, private sector entities, contractors or other external third parties with whom information is shared. Also explain how the disclosure will comply with applicable laws, regulations, and policies. Provide examples on how PII is likely to be disclosed through the agency's activities. Describe any routine information sharing conducted with these external agencies or parties, and how such external sharing is compatible with the original purpose of the collection of the information. Explain how the information is accessed and used, and provide details on any Memorandum of Understanding (MOU), contract or other agreement that govern the sharing of information in the system and whether there are limitations on re-dissemination. Note that information shared with external entities must be compatible with the purpose and use as stated in the applicable Privacy Act system of records notice.

For Privacy Act systems, describe how an accounting of disclosures made outside DOI is maintained. See the Privacy Act, 5 U.S.C. 552a (c) for requirements to account for records disclosed to external parties. DI-3710 Disclosure Accounting form should be used to record the date, nature and purpose of each disclosure from a Privacy Act systems of records, and the name and address of the individual or agency to whom the disclosure is made.

4.2 What safeguards will be in place to prevent uses beyond those authorized under law and described in this PIA?

Describe the security controls and safeguards established to ensure that PII is accessed and used only as permitted by law. These may depend on how the PII is maintained and where. Be sure to include all safeguards for PII collected and maintained by DOI. Describe how DOI will limit access to the PII, whether and how DOI will use encryption or other technical methods to secure the PII, and what steps are taken to reduce the volume of PII to the minimum necessary to accomplish the agency's purposes. For example, are there auditing features, access controls, or other possible technical and policy safeguards such as information sharing protocols, or special access restrictions.

SECTION 5: Maintenance and Retention of PII

5.1 How will the agency maintain the PII, and for how long?

Describe how PII will be maintained and how long it will be retained. Identify any records retention schedule that applies to Federal records that are maintained by, or on behalf of, the agency, and explain retention and disposition methods. Note that any system that contains Federal records must have a NARA approved records retention schedule. Be sure to explain whether all the information is retained or if there are specific subsets of information that are retained, and how subsets of information are deleted. Also include records retention schedules for different types of information or subsets of information.

5.2 Was the retention period established to minimize privacy risk?

If PII is maintained, identify the records retention schedule and provide an explanation on how the retention period minimizes privacy risk. DOI must secure information collected and maintained, and assure its accuracy and integrity so records schedules should align with the stated purpose of the system while retaining PII for the minimum amount of time necessary to meet the requirements of the Federal Records Act.

SECTION 6: How the Agency will Secure PII

6.1 Will privacy and security officials coordinate to develop methods of securing PII?

Describe how privacy and security officials work together to secure PII. Consult government-wide policies that pertain to information security, such as NIST, OMB, and the CIO Council. For example, NIST recommends that organizations take steps to protect their PII, including the following:

- Encourage close coordination among chief privacy officers, senior agency officials for privacy, chief information officers, chief information security officers, and legal counsel when addressing issues related to PII
- To protect PII effectively, organizations need a comprehensive understanding of their information systems, information security, privacy, and legal requirements.
- Decisions regarding the applicability of a particular law, regulation, or other mandate should be made in consultation with the organization's legal counsel and privacy officer since the laws, regulations, and other mandates are often complex and may change over time.
- Consider new technical security controls to enforce new security policies that are adopted.

6.2 How will the agency secure PII? Describe how the agency will limit access to PII, and what security controls are in place to protect the PII.

Describe the security controls and safeguards established to ensure that PII is accessed and used only as permitted by law. Describe how DOI will limit access to the PII, whether and how DOI will use encryption or other technical methods to secure the PII, and what steps are taken to reduce the volume of PII to the minimum necessary to accomplish the agency's purposes.

Privacy risks may be inherent in the sources or methods of collection, or the quality or quantity of information. Describe auditing features, access controls, and other possible technical and policy safeguards such as information sharing protocols, or special access restrictions. Do users have "read-only" access while others are permitted to make certain amendments or changes to the information? Does the IT system have automated tools to indicate when information is inappropriately accessed, retrieved or misused? Describe what privacy and security training is provided to system users. Other security controls may include rules of behavior, encryption, secured facilities, firewalls, etc.

SECTION 7: Identification and Mitigation of Other Privacy Risks

7.1 What other privacy risks exist, and how will the agency mitigate those risks?

Describe other privacy risks associated with the use of the third-party website or application, and how DOI will mitigate those risks. For example, explain how the use of an application implicates geolocation privacy for mobile device users. Privacy notices posted on the third-party site may inform users of the associated privacy risks, and may warn user to avoid disclosing any sensitive PII when interacting with the agency on the site. The use of tracking technology such as "cookies,"

"web bugs," or "web beacons" may also create privacy risks as these technologies can create or develop a history or profile of the user's activities.

7.2 Does the agency provide appropriate notice to individuals informing them of privacy risks associated with the use of the third-party website or application?

Notice can be provided to users through various means, such as the DOI Privacy Policy, DOI Social Media Policy, Privacy Notices posted on third-party websites or applications, or completed privacy impact assessments. Describe how notice is provided to users of the third-party website or application.

SECTION 8: Creation or Modification of a System of Records

8.1 Will the agency's activities create or modify a "system of records" under the Privacy Act of 1974?

Describe any use of the third-party website or application that is subject to the requirements of the Privacy Act of 1974. For all collections of PII where the information is retrieved by a name or other personal identifier, the Privacy Act requires that the agency publish a SORN in the *Federal Register*. The Privacy Act requires that amendments to an existing system must also be addressed in a *Federal Register* notice (see 383 Departmental Manual 5.3).

DOI has developed DOI-08, Social Networks system of records to allow DOI to interact with the public using third-party or social media applications for the purpose of facilitating communication and sharing ideas, disseminating information on upcoming events, notification of emergency or breaking news, soliciting feedback on programs or initiatives, or to improve services to the public. It is DOI policy to limit the collection of PII on individuals to that necessary to accomplish the DOI mission. In the case where records on individuals are created from the use of social media applications, they must be protected, maintained and used in accordance with DOI-08, or other published system of records notice, and all applicable laws, regulations and DOI policy. DOI-08 may be viewed at: http://www.gpo.gov/fdsys/pkg/FR-2011-07-22/html/2011-18508.htm.

The Privacy Act contains criminal penalties for operating a system of records without publishing a system of records notice. Any officer or employee who knowingly and willfully maintains a system of records 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, and be subject to disciplinary action.

8.2 Provide the name and identifier for the Privacy Act system of records.

Provide the name and identifier for the Government-wide, DOI or Bureau/Office Privacy Act system of records notice and the *Federal Register* citation (e.g., XX FR XXXX, Date), and provide a link to the notice.

The Following Officials Have Approved this Document

1) **System Manager**

_____ **(Signature)** _____ **(Date)**
Name:
Title:

2) **Chief Information Security Officer**

_____ **(Signature)** _____ **(Date)**
Name:
Title:

3) **Privacy Officer**

_____ **(Signature)** _____ **(Date)**
Name:
Title:

4) **Reviewing Official**

_____ **(Signature)** _____ **(Date)**
Name:
Title: