Privacy Impact Assessment

Please complete this form if collecting or maintaining information from the general public, Federal personnel and/or Federal contractors, and Volunteers.

Introduction

[This section needs to be re-written into plain language and edited for brevity.] 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.

Section 1. Project Information

Name of Project

Date

Bureau/Office

Bureau/Office Contact Title

Point of Contact's First Name

Middle Name

Last Name

Contact's Email

Phone

Address

City

State/Territory

Zip

Section 2. Description of the System

A. Provide a non-technical overall description of the system that addresses the following:

The response should be written in plain language and should be as comprehensive as necessary to describe the system. If it would enhance the public's understanding of the system, please include system diagram(s).

(1) the purpose that the records and/or system are designed to serve

(2) the way the system operates to achieve the purpose(s)

(3) the type of information collected, maintained, used, or disseminated by the system

(4) who has access to information in the system

(5) how information in the system is retrieved by the user

(6) how information is transmitted to and from the system

(7) whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)

(8) whether it is a general support system, major application, or other type of system.

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

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

UUI Code	Systems Security Plan (SSP) name

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

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