Privacy Impact Assessment (PIA)
for the

International Resource Information System (IRIS)
October 19, 2023

For PIA Certification Updates Only: This PIA was reviewed on Enter date by Name of reviewer certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Garrett Schiche/Education Research Analyst
Contact Email: Garrett.Schiche@ed.gov

System Owner

Name/Title: Garrett Schiche/Education Research Analyst
Principal Office: Office of Postsecondary Education (OPE)

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

The International Resource Information System (IRIS) consists of a grant reporting and management database and a public-facing informational website for the International and Foreign Language Education (IFLE) office within the U.S. Department of Education's (Department) Office of Postsecondary Education (OPE). The IFLE office administers the Higher Education Act of 1965 Title VI (Title VI) and Fulbright-Hays grant and fellowship programs that strengthen foreign language instruction, area/international studies teaching and research, professional development for educators, and curriculum development at the graduate and postsecondary levels.

Under Title VI, IFLE administers the following ten domestic programs that provide a variety of grants to institutions of higher education (IHE) and individuals for projects in foreign languages, area or international studies, and international business:

1. American Overseas Research Centers
2. Centers for International Business Education
3. Foreign Language and Area Studies Fellowships
4. International Research and Studies
5. Language Resource Centers
6. National Resource Centers
7. Undergraduate International Studies and Foreign Language
8. Institute for International Public Policy
9. Business and International Education
10. Technology Innovation and Cooperation for Foreign Information Access

Under the Fulbright-Hays Act, IFLE administers four overseas programs that provide a variety of grants to individuals and institutions for projects in foreign languages and area studies. These overseas grant programs are:

1. Fulbright-Hays Doctoral Dissertation Research Abroad (DDRA)
2. Fulbright-Hays Group Projects Abroad
3. Fulbright-Hays Seminars Abroad - Bilateral Projects

4. Fulbright-Hays Faculty Research Abroad (FRA)

IRIS is used to administer these programs, disseminate information about all IFLE grant programs to the international education community and the general public, and provide publicly accessible records of current and past IFLE grantees. IRIS is also the mechanism by which current IFLE recipients submit required annual/final performance reports (APR) to the Department for oversight and monitoring.

IRIS grant records originate in the Grants Management System (G5), a component of Education's Central Automated Processing System (EDCAPS). EDCAPS is responsible for all grants' pre- and post-award processing, including grant payment processing. Each month, G5 records for each IFLE program are exported into an Excel spreadsheet which is then uploaded into IRIS to populate and update the grantee award record. The G5 extract includes the following:

- applicant's award number, institution name, and address
- applicant's project director's name, email, phone number, fax number, and address
- applicant's project coordinator's name, email, and phone number
- applicant's award budget data
- educational information (including research topics, abstracts, languages studied, and courses taken) and institution affiliation

The IRIS grants management database contains grant-specific data from both IHEs representatives and individual students including names, email addresses, phone numbers, academic programming, and related activities, and budget tracking and performance measurements. Grantees use the database to submit this information as well as reports required by their grant programs, which IFLE staff are able to review and monitor. The system also facilitates dispositions of processes such as general travel plans for grantees, grant activation, grant extension requests, grant hiatus, and research approval.

The public-facing informational website contains basic information about IFLE's international education programs, frequently asked questions, and user support through a "Contact Us" page. It also contains a "Search" function that allows the general public to search for and identify grant award information that is made publicly available for award transparency purposes.

Furthermore, IFLE will be using Microsoft Forms to conduct the Survey of Post-Graduate Employment for the Foreign Language and Area Studies (FLAS) program. The

FLAS program awards grants to IHEs to fund fellowships in foreign language and area studies to students.

IFLE will conduct a survey to collect information about the postgraduate employment, education, or training of FLAS fellows, the global competencies (including language skills and area studies knowledge) acquired during their fellowship, and the extent to which receiving a FLAS fellowship may have contributed to the forementioned. A longitudinal tracking of fellows to measure long-term postgraduate employment, education, or training outcomes is necessary to adequately assess the contribution of FLAS fellows to meeting the demand for language and area studies experts in areas of national need.

1.2. Describe the purpose for which the personally identifiable information (PII)[1] is collected, used, maintained, or shared.

IFLE collects or uses PII in IRIS for the following categories:
- From individual grantees: Grantee name, personal/institutional email address, phone number, address, award number, institution name, award budget data, educational information (including research topics, abstracts, languages studied, and courses taken), institution affiliation, and IRIS login password; project director's name, email, phone number, fax number, and address; and project coordinator's name, email, and phone number.
  - This information is used to create individual user profiles and grant records. The grant records (e.g., annual performance reports, and approval requests) are used to generate periodic grantee progress reports and approve certain requests such as travel. The grant records are accessed by IFLE staff for grant oversight purposes. Institutional representatives also access individual grantee grant records to input performance data such as language proficiency assessment results. The information (award number, institution name, project director name, email address, and phone number) is also used via the public-facing "Search" function in IRIS to search for and identify grant award information that is made publicly available for award transparency purposes.
- From institution representatives: Name, personal/institutional email address, institution affiliation, phone number, fax number, and IRIS login password.
  - This information is used to create institutional user-profiles and grant records. The grant records are used to generate periodic grantee progress reports, which are accessed by IFLE staff for grant oversight. The

---

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

information (award number, institution name, project director name, email address, and phone number) is also used via the public-facing "Search" function in IRIS to search for and identify grant award information that is made publicly available for award transparency purposes.

- From Federal employees and contractors: Name, email address, phone number, and IRIS login password.
    - o This information is used to create IRIS user profiles for IFLE staff and contractors. None of this information is made publicly available.
- From the "Contact Us" form: Name, email address, award number (optional), and message.
    - o This information is used to log and respond to inquiries about IRIS from grantees and the general public.

For the FLAS survey, IFLE collects information from individual FLAS fellows for the following purposes.

- Administration: Information is needed to send the survey to the respondents and track who has completed the survey to ensure a response rate that sufficiently addresses non-response bias. This requires collecting the following PII:
    - o Name, personal phone number, and personal email address.
- Longitudinal tracking: The FLAS Survey is a longitudinal survey that requires tracking individual respondents from one survey to the next. This requires collecting the following PII:
    - o Name, personal email address, gender, educational background, employment information, and race.
- Outcome analysis: The FLAS Survey is required to gather information on long-term outcomes of the FLAS program, focusing on employment. It also seeks to understand if there are any disparities in outcomes that are linked to gender, race/ethnicity, or educational background. This requires collecting the following PII:
    - o Name, personal phone number, personal email address, gender, race/ethnicity, and educational background.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

The PIA is being updated as part of the required biennial review.

1.5. Is the system operated by the agency or by a contractor?

Contractor

    1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

       ☐ N/A

       Yes

2. Legal Authorities and Other Requirements
If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include the name and citation of the authority.

IRIS

The information is collected under the legal authority of The Higher Education Act of 1965, as amended, Part A, Title VI, section 605(a) and (b), which offers domestic grants to IHEs to develop and maintain capacity and performance in area/international studies and world languages and the Mutual Educational and Cultural Exchange Act of 1961, as amended (22 U.S.C. 2451–2458) (commonly known as the Fulbright-Hays Act), which provides funding to current and prospective U.S. educators to participate in advanced overseas study and research.

FLAS

FLAS is a survey of fellows required by 20 U.S.C. §1121(d) which states, "The Secretary shall assist grantees in developing a survey to administer to students who have completed programs under this subchapter to determine postgraduate employment, education, or training. All grantees, where applicable, shall administer such survey once every two years and report survey results to the Secretary."

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

When logged into IRIS, IFLE staff and grantee representatives can access grantee records (institutional and individual) by award number, institution name, individual

grantee name, and/or email address. Grant records are most often retrieved via award number and institution name, but records can also be accessed via institution or individual grantee names.

The public-facing IRIS website allows information to be retrieved by institution name, grantee State, and fellow (individual grantee) first and last name. When a record is identified, all information entered into the grantee record is displayed, both institutional and individual records, apart from approval requests. For the FLAS, each respondent will be assigned a number in the order of submitting responses in Microsoft Forms.

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[2] Please provide the SORN name, number, Federal Register citation, and link, or indicate that a SORN is in progress.
☐ N/A

The following SORNs cover the IRIS system:
- "[Fulbright-Hays – Doctoral Dissertation Research Abroad (DDRA) and Seminars Abroad (SA)](#)," 18-12-02, 84 FR 40033, was published in the Federal Register on August 13, 2019.
- "[Title VI International Research and Studies Program (IRS)](#)," 18-12-04, 83 FR 13263, was published in the Federal Register on March 28, 2018.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.
☑ N/A

Records Management
If you do not know your records schedule, please consult with your records liaison, or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

---

[2] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

For unsuccessful grant applications:
General Records Schedule (GRS) 1.2, item 021 Grant and cooperative agreement case files, Unsuccessful applications.
Temporary. Destroy 3 years after final action is taken on file, but longer retention is authorized if required for business use.

For general grant deliverables:
General Records Schedule (GRS) 1.2, item 030 Final grant and cooperative agreement products or deliverables.
Temporary. Destroy when business use ceases.

For grant deliverables with historic or long-term value, such as completed research or studies, and the FLAS Survey:
ED 254 Grant Administration and Management Files (N1-441-11-1), item E2, Historically Significant Products.
Permanent. Transfer to the National Archives.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

IFLE collects PII in the following categories for IRIS:
- From individual grantees: Grantee name, personal/institutional email address, phone number, address, award number, institution name, award budget data, educational information (including research topics, abstracts, languages studied, and courses taken), institution affiliation, and IRIS login password; project director's name, email, phone number, fax number, and address; and project coordinator's name, email, and phone number.
- From institution representatives: Name, personal/institutional email address, institution affiliation, phone number, fax number, and IRIS login password.
- From Federal employees and contractors: Name, email address, phone number, and IRIS login password.
- From the "Contact Us" form: Name, email address, award number (optional), and message.

IFLE collects PII in the following categories in the FLAS Survey:
- From individual FLAS Fellows: Name, personal phone number, personal email address, gender, educational background, employment information, and race.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

The PII collected and maintained is the minimum amount required by IRIS to track and administer its programs and to establish user accounts to access the IRIS system for reporting purposes. IRIS collects individual grantee contact information in the event the grantees need to be contacted as a result of a grant being approved. IFLE needs to contact grantees by telephone, email, or fax. In addition, IFLE needs to collect login information to establish accounts for each group of IRIS users. Finally, IFLE uses IRIS to manage grants and to allow grantees to meet reporting requirements necessary to receive grant funding. IFLE needs basic information about grants (e.g., grantee name, institutional affiliation, research area, and budget information) to fulfill this function.

For the FLAS survey, the PII collected and maintained is the minimum amount required for the administration of the survey, for longitudinal tracking, and for outcome analysis. Participation is voluntary and there are no consequences if an individual chooses not to participate or not to respond to specific questions on the survey.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

IRIS
PII is submitted by individual grantees and individuals assigned by institutions to manage their grant awards (obtained by IRIS via the G5 system or directly from individuals and institutions). In addition, IFLE staff create IRIS user profiles (including login information) for IFLE staff and contractors.

FLAS Survey
All PII is entered by FLAS fellow survey respondents.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

IRIS

PII is transmitted from the G5 system to initially populate grantee records or entered directly into IRIS by individual grantees or individuals assigned by institutions to manage their grant awards.

FLAS Survey

PII is collected via the FLAS survey that is implemented using Microsoft Forms.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[3] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

IRIS

For G5, payees are vetted via the external payee access form submitted by the user accompanied by a letter with the school letterhead requesting the access and verified by a school supervisor. Once information is transferred from G5 to IRIS, individuals are responsible for ensuring the accuracy of their information. Individuals may contact the help desk to correct any inaccurate information.

Additionally, there are controls that validate the information, including not allowing the submission of information unless all required sections are completed. For programs that have both institutional record owners and individual grantees (i.e., FLAS, DDRA, FRA), only the institutional record owners are allowed to submit final approval for individual grantee records or reports. This is a data quality mechanism that requires institutions to validate the accuracy of individual grantee records or reports before they are officially submitted to IRIS for review by IFLE staff.

FLAS Survey

The link to the FLAS survey is sent out by university FLAS coordinators who have a list of all fellows with contact information. Only fellows who receive the link can fill out the survey. Fellows enter their PII at the end of the FLAS Survey and are prompted to review their PII to ensure its accuracy before final survey submission.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

IRIS

---

[3] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

The PII is used to query, update, and track institutional and individual grantee records in IRIS. It is also used to approve requests for things such as award extensions, foreign language selections, and individual grantee travel. Each individual grantee can also be linked to an institution; this is used to ensure that individual grantee approvals do not exceed institutional allocations.

The PII is also used via the public-facing "Search" function in IRIS to search for and identify grant award information that is made publicly available for award transparency purposes.

FLAS Survey

In the FLAS survey IFLE collects PII from individual FLAS fellows for the following purposes.

- Administration: PII is needed to track who has completed the survey to ensure a response rate that sufficiently addresses non-response bias. This requires collecting the following PII.
  - Name, personal phone number, personal email address.
- Longitudinal tracking: The FLAS Survey is a longitudinal survey that requires tracking individual respondents from one survey to the next. This requires collecting the following PII:
  - Name, personal email address, gender, educational background, employment information, and race.
- Outcome analysis: The FLAS Survey is required to gather information on long-term outcomes of the FLAS program, focusing on employment. It also seeks to understand if there are any disparities in outcomes that are linked to gender, race/ethnicity, or educational background. This requires collecting the following PII:
  - Name, personal phone number, personal email address, gender, race/ethnicity, and educational background.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?
☑ N/A

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

No

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.
☑ N/A

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.
☑ N/A

4. Notice
4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

IRIS
IRIS grant records originate in the G5 system, a component of EDCAPS. EDCAPS is responsible for all grants' pre- and post-award processing, including grant payment processing. Each month, G5 records for each IFLE program are exported into an Excel spreadsheet which is then uploaded into IRIS to populate and update the grantee award record. Notice is provided by the G5 system when a grant is approved for an institution. For additional information related to the notice provided by the G5 system, please refer to the EDCAPS PIA, located on the [Department PIA website](). Once information is populated within IRIS, accounts for institutions are created by the IRIS administrator. When institutions then award grants to individuals (FLAS, DDRA, FRA), individuals provide their information to the institutions and that information is then entered into IRIS to establish an individual grant record by the institution. Additionally, notice is provided by the SORNs referenced in section 2.2.1.

FLAS Survey
A Privacy Act Statement is provided on the landing page of the survey that respondents must review before moving forward to the rest of the survey.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

IRIS

For additional information related to the notice provided by the G5 system, please refer to the EDCAPS PIA, located on the [Department PIA website](#).

FLAS Survey

Authority: The Foreign Language and Area Studies (FLAS) Fellowships program is authorized by 20 U.S.C. §1122(b) and provides allocations of academic year and summer fellowships to IHEs or consortia of IHEs to assist meritorious undergraduate and graduate students undergoing training in modern foreign languages and related area or international studies. This is a survey of FLAS fellows required by 20 U.S.C. §1121(d) which states "The Secretary shall assist grantees in developing a survey to administer to students who have completed programs under this subchapter to determine postgraduate employment, education, or training. All grantees, where applicable, shall administer such survey once every two years and report survey results to the Secretary."

Purpose: The purpose of the survey is to collect information about the postgraduate employment, education, or training of FLAS fellows, the global competencies (including language skills and area studies knowledge) acquired during their fellowship, and the extent to which receiving a FLAS fellowship may have contributed to the forementioned. Your responses will contribute to the design of improved Federal student assistance programs.

Disclosures: Your answers to this survey are confidential and anonymous, and no individual responses can be identified or traced. Only aggregate measures of the responses to this survey will made available to the public. For examples of how the results from this survey may be shared, please see the [International and Foreign Language Education FLAS Performance](#) website for previous survey reports.

Consequences of Failure to Provide information: Your participation is voluntary and there are no consequences if an individual chooses not to participate or not to respond to specific questions on the survey.

The International and Foreign Language Education (IFLE) Office at the Department of Education thanks you for participating in this study. We rely on your accurate responses on this survey to report correctly on the outcomes of this program.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

IRIS

Providing information to IRIS is voluntary. Institutions and individuals have the opportunity to decline to provide the information; however, providing certain information is required to create accounts for meeting reporting requirements necessary to receive grant funding.

FLAS Survey

Completing the FLAS Survey is voluntary. There are no consequences if an individual does not wish to participate in the survey.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

No

5.2. What PII will be shared and with whom?
☑ N/A

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?
☑ N/A

External

5.4. Will the PII contained in the system be shared with external entities (e.g., another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.
IRIS
Yes

FLAS Survey
No

5.5. What PII will be shared and with whom? List programmatic disclosures only.[4]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.
☐ N/A

IRIS
The names and contact information of grant recipients (institution directors or individual grantees) and information about their projects, such as dissertation subjects, are publicly available on the website for people researching grants.

5.6. What is the purpose for sharing the PII with the specified external entities?
☐ N/A

IRIS
The purpose of posting the information is for oversight and transparency regarding the use of public money, and research purposes.

5.7. Is the sharing with the external entities authorized?
☐ N/A

IRIS
Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?
☑ N/A

5.9. How is the PII shared with the external entity (e.g., email, computer match, encrypted line, etc.)?
☐ N/A

IRIS
PII is made available through the public-facing "Search" page on the IRIS webpage.

---

[4] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☑ N/A

Click here to select.

5.11. Does the project place limitation on re-disclosure?

☐ N/A

IRIS

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

IRIS

All IRIS users can access and update the information they entered into their grantee record by logging into IRIS. All users can also access completed grantee record information via the public-facing "Search" site of IRIS.

Additionally, if an individual wishes to gain access to records regarding them in this system of records, contact the system manager at the address listed in the SORNs referenced in question 2.2.1. Requests must contain the necessary particulars, such as full name, date of birth, the year of the award, the name of the grantee institution, the major country in which the educational activity was conducted, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. The request must meet the requirements of the regulations at [34 CFR 5b.5](#).

FLAS Survey

In addition to the above statement, FLAS fellow survey respondents can contact the FLAS program officer to review their responses if necessary.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

IRIS

IRIS users can update their password within IRIS but must contact IRIS administrators to update their username (email address). IRIS users must also contact IRIS

administrators to update PII in grantee records that have already been submitted and approved by the Department. Contact information for the IRIS system is provided on the IRIS website.

Additionally, if an individual wishes to contest the content of a record regarding them in this system of records, contact the system manager at the address listed in the SORNs referenced in question 2.2.1. Requests should contain full name, date of birth, the year of the award, the name of the grantee institution, the major country in which the educational activity was conducted, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. The request must meet the requirements of the regulations at 34 CFR 5b.7.

FLAS Survey
In addition to the above statement, FLAS fellow survey respondents can contact the FLAS program officer to update their responses or correct erroneous data if necessary.

6.3. How does the project notify individuals about the procedures for correcting their information?

IRIS
Grantees can find information on how to correct their PII in the FAQs on the IRIS page, via new grantee orientations conducted by program officers, or via helpdesk support. In addition, this PIA, as well as the system of records notice listed in question 2.2.1, details the procedures for correcting information.

FLAS Survey
In addition to the above statement, procedures for correcting information are providing on the survey landing page.

7. **Safeguards –** The following responses are only applicable to IRIS as the FLAS Survey is conducted using MS Forms.
If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?
Yes

7.2. Is an Authorization to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

| Moderate |

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

IRIS resides on a cloud server (Department Amazon Web Services - East-West Cloud) that is a FedRAMP-compliant (a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services) hosting provider and is required to meet Department security requirements, including those related to physical access to the facility. All physical access to the Department's site where this information is maintained is controlled and monitored by security personnel who check everyone entering the building for his or her employee or visitor badge. All users access the system through an email address and a unique password.

Access to the system is limited to authorized IRIS program personnel and contractors responsible for administering the IRIS program. Authorized personnel include Department employees and contractors who have responsibilities for implementing the IRIS program.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), IRIS must receive a signed ATO from a designated Department official. FISMA controls implemented by IRIS are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO), are required to read, and accept a Rules of Behavior and are required to utilize a complex password and two-factor authentication.

The IRIS server has additional security measures in place. Authentication to the server is done via an encrypted virtual private network tunnel. A hardware firewall is in place and no other machines reside on the internal firewall network except for the IRIS server.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

| Yes |

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing, or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

The system administrator runs required scans/tests on a monthly and annual basis as required. Security and system documentation is updated as required. Monitoring and auditing of all event logs are performed on a regular basis. Patches are checked for on a periodic basis and tested and applied to the server on a weekly basis, depending on necessity.

When going through the ATO/Ongoing Security Authorization (OSA) process, the system owner establishes monitoring processes to ensure the information is used in accordance with the approved practices. During the OSA process, smaller subsets of security controls are tested every quarter.

8. **Auditing and Accountability**
   8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures that the information is maintained and used in accordance with the stated practices in this PIA. The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, IRIS makes sure that the National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls comprise of administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings and meets regularly with the ISSO.

   8.2. Does the system owner/program officer continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

Privacy risks associated with IRIS include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include embarrassment or loss of credentials that are used to gain access to other resources. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by updating security patches and updating devices' operating software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.