Privacy Impact Assessment

For IRIS

Date: April 29, 2010

Point of Contact, System Owner, Author: Karla Ver Bryck Block

Office of Postsecondary Education
U.S. Department of Education

1. System Information. Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

The International Education Programs Service (IEPS) within the Office of Postsecondary Education, U.S. Department of Education (ED) manages 14 grant and fellowship programs. It has developed a Web-based database that is used in conjunction with managing these 14 programs and disseminating information about them. The International Resource Information System (IRIS) contains publicly accessible records of current and past IEPS grantees and is a dissemination mechanism for information about all IEPS grant programs to the international education community and to the public as a whole. It also contains a grantee-only password protected reporting feature that captures and reports Annual/Final Performance Reports (APR) from current IEPS grantees.

2. **Legal Authority. Cite the legal authority to collect and use this data.** What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

EDGAR 74.51 requires grantees to submit performance reports to US/ED. Also, the performance reports are required as part of the terms and conditions of the grant award (Attachment B). IEPS collects these reports through IRIS.

3. **Characterization of the Information. What elements of PII are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)?** What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

IRIS collects the names of individuals who receive grant funds for direct benefit. Individuals who receive grant funds from institutional awards (i.e., travel awards, per diem, etc) have their names stored in IRIS as recipients of the funds. Individuals who receive fellowships from IEPS through an institution have their names listed on the public side of IRIS. These lists contain the same information that is posted on www.ed.gov regarding IEPS fellowship recipients. There is no linking or cross-referencing.

4. **Why is the information collected? How is this information necessary to the mission of the program, or contributes to a necessary agency activity**. Given the amount and any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

EDGAR 74.51 requires grantees to submit performance reports to US/ED. IEPS collects reports through IRIS. The reports are reviewed by program staff to ensure grantee compliance and to assess performance. No privacy risks have been identified.

5. **Social Security Numbers - If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures.** Also specify any alternatives that you considered, and why the alternative was not selected.

SSNs are not collected.

6. **Uses of the Information. What is the intended use of the information?** How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to

analyze the data? If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

Internal uses include using the information for monitoring the grants and conducting daily grant administration actions such as time extensions, travel approvals, foreign language approvals, overseas program approvals.

Data sets are available on the public side of IRIS and these are used by grantees as well as research organizations to conduct program analyses and evaluations. Program descriptions are available for public viewing in IRIS in order to disseminate grant information.

7. **Internal Sharing and Disclosure. With which internal ED organizations will the information be shared?** What information is shared? For what purpose is the information shared?

Budget and performance information from IRIS is used by Budget Service and Strategic Planning Services (OPE) to write budget justifications and conduct analyses.

8. **External Sharing and Disclosure. With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)?** What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding or other type of approved sharing agreement with another agency?

Data sets are available on the public side of IRIS and these are used by grantees as well as research organizations to conduct program analyses and evaluations. Project abstracts are shared as a means to disseminate grantee information to the public.

9. **Notice. Is notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)?** What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

Yes. IRIS is cleared by the Office of Management and Budget as the sole reporting instrument for the 14 IEPS programs. Required fields in IRIS are marked by an asterisk; those fields without an asterisk are voluntary.

10. **Security. What administrative, technical, and physical security safeguards are in place to protect the PII?** Examples include: monitoring, auditing, authentication, firewalls, etc. Has a C&A been completed? Is the system compliant with any federal security requirements?

The last IRIS C&A was on August 2007.

Monitoring/Auditing of all Windows Server event logs are performed on a regular basis. Microsoft Baseline Security Analyzer is used on periodic basis to check for any missing patches or other issues. Patches are tested and applied to the server on a weekly basis, depending on necessity. Authentication to the server is by encrypted VPN tunnel. A hardware firewall is in place to block all unnecessary ports going to the server. No other machines reside on internal firewall network except for IRIS server.