Privacy Impact Assessment

For

Office of Indian Education - Professional Development Grants Performance and Results Act and Service Payback Data Collection System

Date: August 8, 2013

Point of Contact: Jim Barthmaier (COR)

System Owner: Joyce A. Silverthorne

Author: Jim Barthmaier

Office of Elementary and Secondary Education

U.S. Department of Education (ED)

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 system is a service obligation tracking system (SOTS) known as the Indian Education Professional Development (IEPD) Grants Performance and Results Act and Service Payback Data Collection System in the Office of Indian Education (OIE). OIE has partnered with the Office of Special Education Programs (OSEP) to develop and maintain the system. The IEPD system will collect data from OIE grantees, participants and employers to track the eligible employment of participants who have received funding from Professional Development Program grants, until their service obligations are fulfilled or they are referred to ED's Debt & Payment Management Group (DPMG) for repayment of part or all of the funding received.

The system will also collect budget and project-specific performance data from grantees. Reports generated will be used by OIE to document information on the characteristics of program participants and the outcomes of the grant projects (program completion, certification, employment in the area supported by training, etc.). Collection of these data attributes is critical in assessing project and program performance and compliance with applicable laws and regulations.

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?

The information is being collected under the authority of section 7122 of the *Elementary and Secondary Education Act of 1965*, as amended (20 U.S.C. 7442), and the implementing regulations at 34 CFR Part 263, Subpart A, as well as with the Government Performance and Results Act of 1993 (GPRA), Section 4.

3. **Characterization of the Information.** What elements of personally identifiable information (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?

Sources of information are program grantees participants, and participants' employers.

The personal identifiable information (PII) collected from participants, from grantees about the participants, and from employers about the participant includes: name, social security number, mailing address, email address, and telephone number(s). The system also collects alternate contact information, which includes name, relationship of person to participant, mailing address, and telephone number(s) of individuals identified by the participant.

For grants awarded before FY 2009, the information is collected via email, mail, and telephone calls with grantees, participants, and employers. The information is maintained in the grantee and participant folders and locked into filing cabinets at Department Headquarters. Program participant PII information captured during the exchange of emails with grantees, participants, and employers may be stored in electronic form on the Department's servers as emails, Word and Excel documents.

For grants awarded between FY 2009 and FY 2012, the information is collected via website, mail, email and telephone calls with grantees, participants, and employers. Some information is collected and stored in grantee and participant folders and some will be collected and stored on a secure server. Depending on the availability of program funds, information stored in paper form will be converted into electronic form and the paper folders destroyed in accordance with Federal disposition requirements.

For grants awarded for FY 2013 and forward, the information will be collected electronically via a secure online website and stored in electronic form only. For those individuals who do not have the technology or internet

access to use the online Web site, information will be collected via mail, email, and telephone and then converted to electronic form and stored in the online system.

The information in this system is not used to link or cross-reference multiple databases, with the exception of the existing paper-based IEPD files. OIE may cross-reference information in the electronic system with information stored in the paper files to identify participants with outstanding payback balances and take appropriate action to get them to fulfill their payback obligation.

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 type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

The information is necessary for three reasons. First, data from all three sources (grantees, project participants, and employers) are necessary to determine if IEPD participants are fulfilling the terms of their service/cash payback requirements. Second, budget and project-specific performance data are collected from IEPD grantees for project monitoring. And finally, data from these three sources are necessary to assess the performance of the IEPD program on its *Government Performance Results Act (GPRA)* measures.

The privacy risks identified were unauthorized access to PII information and the use of SSNs in the electronic database. These risks have been mitigated through privacy training for both contractor and Department staff and restricting access to PII data to a select few individuals that have a direct business need for the information. Additionally, to protect participants' SSNs the database will create a unique identifier for each program participant that will be used for database activities. The SSN will only be accessed when a participant does not fulfill their service payback obligation and a cash payback referral is made to DPMG, when there is a need to use a unique identifier to identify participants because of duplicate names, and to determine whether participants have received funding from multiple grants to ensure all payback requirements have been met for each participant.

5. **Social Security Numbers (SSN).** 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. If system collects SSN, the PIA will require a signature by the Assistant Secretary or designee. If no SSN is collected, no signature is required.

The purpose of collecting social security numbers is to ensure that participants repay funds in the event service payback cannot be completed. Participants who cannot complete a service payback are required by law to provide a cash payback. The DPMG and the U.S. Department of Treasury require social security numbers to confirm identity and to provide to the Internal Revenue Service for collection purposes should a participant default on cash payback. There are no alternatives possible for this purpose.

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? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

The information is used to monitor compliance by participants in meeting their service and/or cash payback obligations, as well as for the other purposes described in question four above.

Descriptive statistical methods are used to compile data for the evaluation of the Professional Development Program performance measures. Data from the Institute of Education Sciences' (IES) Common Core of Data System will be used in conjunction with data collected by SOTS to calculate results for program performance measures relating to the percentage of graduates employed in targeted schools.

Information from the Department's grants database, G5, is used to pre-populate fields of the web-based data collection system to decrease the burden for grantees.

No commercial information or publicly available information is used.

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?

Information about specific individuals such as name, address, telephone number, training history, and amount of funding received are shared by the Office of Indian Education with ED's DPMG only when a participant defaults on both service payback and cash payback as required. The information allows DPMG to contact the participant and make arrangements to complete a cash payback of all or a prorated amount of the funding provided to the participant by the program.

Per Office of Management & Budget (OMB), program data may be made available to the Department's Institute of Education Sciences for the purpose of program evaluation; however, no PII will be shared as part of the program evaluation data sharing. Data compiled in statistical form and without PII may also be shared with ED officials upon request for program oversight purposes.

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?

If the DPMG is unable to contact a participant after repeated efforts, or has a participant that has defaulted in making cash payments, the personal information is forwarded to the Department of Treasury for collections as required by Federal law. The information that may be shared include the participant's name, address, telephone number, length of time in training, total amount of funding received, prorated balance to be repaid, and employment information to include the name, address, and telephone number of previous employers.

Each participant signs a payback agreement when enrolled in the program which explains the service and cash payback requirements. By signing the agreement the participant demonstrates their understanding that a service or cash payback will be required after graduation or upon exiting the program. Should the participant default on a repayment plan or be non-responsive to the Department's request for repayment, participant information is forwarded to the Department of Treasury for collections.

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?

Participation in the program is voluntary. All participants sign a payback agreement upon entering the program, that explains that a payback in service or in cash is a requirement upon graduation or exiting the program. This agreement provides notice to the participant of the requirements as well as the amount of funding received.

A copy of the Privacy Notice will be posted online at the web address specified in question 10 and will be easily accessible by anyone using the online system.

10. **Web Addresses.** List the web addresses (known or planned) that have a Privacy Notice.

http://pdp.ed.gov/oie/privacysecurity (planned)

11. **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?

Office of the Chief Information Officer (OCIO) is currently conducting an assessment of the electronic system and will issue an authorization to operate (ATO) once the system has meet all federal security requirements.

The system will comply with all IT security requirements in the Federal Information Security Management Act (FISMA) www.csrc.nist.gov/sec-cert/index.html , OMB Circulars www.whitehouse.gov/omb/circulars/index.html, and the National Institute of Standards and Technology (NIST) standards and guidance www.nist.gov.

The system will be monitored continuously by the contractor and security scans will be conducted and provided to (OCIO at least quarterly. All vulnerabilities identified during these scans will be documented and resolved in accordance with Federal requirements.

For participant information stored in paper files, the privacy risks are mitigated by storing information under lock and key at headquarters in Washington, DC. Only program staff with the requisite privacy training has access to these files.

For participant information stored electronically, the online system has had extensive security testing and meets all security requirements for the moderate level.

12. **Privacy Act System of Records.** Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

An existing system of records is being revised to reflect several new data items to be collected and the change from a paper-based to electronic system of record.

This is an Office of Indian Education only system – not a Department or Federal Government-wide SORN.

13. **Records Retention and Disposition.** Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number.

The records contained in this system will be maintained and disposed of in accordance with the records retention and disposition authority approved by the National Archives and Records Administration (NARA). Until NARA approves a retention and disposition schedule for these records, the Department will not destroy or delete any records.