Privacy Impact Assessment (PIA)
for the
Personnel Development Program Data Collection System (PDPDCS)

This PIA was approved on [Sep 27, 2017] and reviewed on [Oct 13, 2017, Oct 25, 2017] by the system owner certifying the information contained here is current and up to date.

Contact Point

Contact Person/Title: Sherron Dunmore, ISSO
Contact Email: sherron.dunmore@ed.gov

System Owner

Name/Title: Bonnie D. Jones, PDPDCS Information System Owner (ISO)
Program Office: Office of Special Education Rehabilitative Services (OSERS)

Reviewing Official
Kathleen Styles
Chief Privacy Officer
U.S. Department of Education

Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division 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.

All text responses are limited to 1,500 characters. If you require more space, please contact the Privacy Safeguards Team.

1. Introduction

1.1 N/A Describe the system including the system name, system acronym, and a brief description of the major functions.

The Personnel Development Program Data Collection System (PDPDCS), an IT system investment, provides for the collection of data from grantees, scholars and their employers to track the enrollment, eligible employment of scholars, and service obligation fulfillment of scholars who have received program funds, until their service obligations are fulfilled or they are referred to the Accounts Receivable and Bank Management Group (ARBMG) for repayment of part or all of the funds received. The PDPDCS also provides technical assistance to all users and generates performance data for reporting annually on program results. The PDPDCS serves the Office of Special Education Programs (OSEP); Rehabilitation Services Administration (RSA); and the Office of Indian Education (OIE). OSEP and RSA use the term "scholar" to refer to individuals who receive financial support from personnel development grants. While OIE uses the term "participant" instead of "scholar," the term "scholar" will be used in this document.

1.2 N/A Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained or shared.

PII is collected, used, and maintained to track the enrollment and service obligation fulfillment of scholars and to refer scholar debt to ARBMG when the scholar's obligation has not been fulfilled through service.

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. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
1.3 □ N/A Is this a new system, or one that is currently in operation?

Currently Operating System

1.4 □ N/A Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.

Updated PIA  
Original Publication Date: 06/01/2014

1.5 □ N/A Is the system operated by the agency or by a contractor?

Contractor

2. Legal Authorities and Other Requirements

*If you are unsure of your legal authority, please contact your program attorney.*

2.1 □ N/A What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?

OSEP: The Government Performance and Results Act of 1993 (GPRA), Public Law 103-62 (requires program performance measurement); Individuals with Disabilities Education Improvement Act (IDEA), Public Law 108-446 (funding a performance measurement); Individuals with Disabilities Education Improvement Act (IDEA), Public Law 108 – 446, (addresses providing personnel development to improve services and results for children with disabilities); Regulations related to these programs can be found at 34 CFR part 304

Office of Indian Education: Public Law 107-110, Title VI, Part A, Subpart 2, Sec. 6122 (20 U.S.C 7442), Regulations 34 CFR 263

Rehabilitation Service Administration: The Rehabilitation Act of 1973, as amended by title IV of the Workforce Innovation and Opportunity Act (WIOA), (requires program performance measurement and authorizes service obligation)

Regulations: 34 CFR 386, CFR 367 et. seq

**SORN**

2.2 □ N/A Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification? Please answer **YES** or **NO**.

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

The current OSEP SORN name is Special Education - Individual Reporting on Regulatory Compliance Related to the Personnel Development Program's Service Obligation and the Government Performance Results Act of 1993 (GPRA). The OSEP SORN number is 18-16-04, published October 24, 2008. The OIE SORN number is 18-14-05, published January 25, 2011. A consolidated SORN is in progress that will include system upgrades and apply to all programs. The updated SORN will include OSEP, RSA, and OIE, and have an updated name, Individual Reporting on Regulatory Compliance Related to the Service Obligation Regulations and the Government Performance Results Act of 1993 (GPRA).

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 N/A Does a records retention schedule, approved by the National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA 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). PDPDCS manages records in accordance with the following records schedule: “Program Management Files,” Schedule Locator 066. The NARA disposition authority is N1-441-10-1.

---

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](https://connected.ed.gov/om/Documents/SORN-Process.pdf)
2.4 N/A Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule? Please answer YES or NO.

Yes

3. Characterization and Use of Information

Collection

3.1 N/A List the specific personal information data elements (e.g., name, email, address, phone number, date of birth, Social Security Number, etc.) that the system collects, uses, disseminates, or maintains.

The information collected, used and maintained consists of records about scholars who receive funding from OSEP, RSA and OIE training grants. Information in this system includes the following for each scholar: name, date of birth, social security number (SSN), personal mailing address, personal phone numbers, financial information on grant funding received, Pre-Scholarship Agreement, Exit Certification (OSEP and RSA only), personal email address, education records, employment status, and place of employment. This information is provided by the grantee and the scholar. Employers verify the employment information provided by the scholar.

3.2 N/A Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2? Please answer YES or NO.

Yes

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

Sources of information are grantees, the scholars, and employers of the scholars. The grantee submits enrollment and educational program data on each scholar. The scholar submits their place of employment, dates of employment, role or position while employed, and information required to determine eligible employment as determined by respective program regulations. The scholar's employer verifies employment data.

For OSEP and OIE, the contractor extracts demographic information on the public school districts from the Department’s Common Core of Data System, to determine if the scholar’s employment after program completion meets criteria established in the program performance measures.
The data are submitted at https://pdp.ed.gov. In rare cases, paper alternative forms may be used.

The information is validated by the grantee who submits a scholar record for each scholar receiving a scholarship; the personal data and enrollment information is reviewed by the scholar; and the employer validates the employment record of the scholar. Random validation of data occurs on a regular schedule by the contractor.

Examples include form filling, account verification, etc.
Use

3.6 □ N/A Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

Information is used to monitor compliance of scholars in meeting their service obligation agreements. When scholars elect or are referred for payback, sensitive information is encrypted and transmitted electronically from PDPDCS to ARBMG.

Descriptive statistical methods are used to compile data for the evaluation of program performance measures. For OSEP and OIE, data from the Institute of Education Science’s (IES) Common Core Data System is used in conjunction with data collected by the PDPDCS to calculate results for program performance measures.

Information from the Department’s grants database, G-5, is used to pre-populate fields of the Web-based data collection system to decrease burden on grantees. No commercial information or publicly available information is used.

3.7 □ N/A Is the project using information for testing a system or for training/research purposes? Please answer YES or NO.

Yes

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

Yes, program level PDPDCS data are used to train grantees on data quality, but are limited to items related to program performance measures. No individual data are used in training to mitigate the risk and protect the data.
3.8 □ N/A Does the system use "live" PII for the development or testing of another system? Please answer YES or NO.

No

3.8.1 □ N/A If the above answer is YES, please explain.

Social Security Numbers

*Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

3.9 □ N/A Does the system collect Social Security Numbers? Please answer YES or NO.

Yes

3.9.1 □ N/A If the above answer is YES, explain the purpose for its collection, and how the SSN will be used. *Please note if the system collects SSNs, the PIA will require a signature by the Assistant Secretary or equivalent.*

Because scholars must fulfill a service obligation in exchange for funding received or repay part or all of the funding received from the grantee, SSNs are required to refer scholars or repayment to ARBMG. If a scholar defaults on payment, ARBMG must provide an SSN when referring the debt to the Department of Treasury. Both ARBMG and the Department of Treasury require SSNs to confirm identity and process the debt. There are no alternatives possible for this purpose.
3.10 □ N/A Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

There are no alternatives possible for this purpose.

4. Notice

4.1 □ N/A How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

As authorized by requirements and regulations, scholars must sign a Pre-Scholarship Agreement, which includes information and resources to ensure that they understand their responsibility for completing a service obligation in exchange for scholarship funding. In addition, they must provide their contact information, date of birth and SSN prior to receiving a scholarship from a Federal grant. The PDPDCS Web site includes the required Privacy Notice. In addition, users must acknowledge the terms of use prior to logging into the Web site. (https://pdp.ed.gov)
4.2 N/A Provide the text of the notice, or the link to the webpage where the notice is posted.

https://pdp.ed.gov/OSEP/home/privacy
https://pdp.ed.gov/OIE/home/privacy
https://pdp.ed.gov/RSA/home/privacy (under development)

4.3 N/A What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

As authorized by requirements and regulations, scholars must sign a Pre-Scholarship Agreement, which includes information and resources to ensure that they understand their responsibility for completing a service obligation. If they do not complete and sign the Pre-Scholarship Agreement, scholars opt out of the program. For OSEP, the Pre-Scholarship Agreement states: "You are advised that your participation in the Office of Special Education (OSEP) Personnel Development Program (PDP) is voluntary and that giving us your student educational information is voluntary, but you must provide the requested information, including your PII, to participate."

5. Information Sharing

Internal

5.1 N/A Will information be shared internally with other ED organizations? Please answer YES or NO. If the answer is NO, please skip to Question 5.4.

Yes
When the Department determines scholars will not fulfill their service obligation and must instead repay some or all of the scholarship they received, the Department sends debt referral information to the Department’s ARBMG.

The Department also uses scholar and employer data for reporting on program performance measures. The results of the performance measures are shared within the program office and with the Department's Budget Services.

Data may be made available to the IES or its contractor for the purpose of program evaluation; however, no PII will be shared as part of program evaluation data sharing. Data compiled without PII may also be shared with ED officials upon request for program oversight purposes.

Yes, the purpose aligns with the stated purpose in Question 1.2. The purpose of sharing information with ARBMG is for debt referral. The purpose of sharing data with IES or its contractor is for the purpose of program evaluation. The purpose of sharing data with ED officials is for the purpose of program monitoring.

External

Yes
5.5 N/A What information will be shared and with whom? Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

Should the scholar default on a repayment plan or be non-responsive to the Department’s request for repayment, scholar information, including SSN, is forwarded by ARBMG to the Department of Treasury for collection. The PDPDCS does not currently share SSNs externally with non-federal entities, and would only do so for a legitimate, authorized purpose, as permitted by a routine use.

5.6 N/A What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

The purposes align with the stated purpose in Question 1.2. The purposes are for 1) sharing information externally when debt is referred to the Department of Treasury for collection; and 2) disclosing information that is under the routine uses listed in the system of records notice. The Department may disclose information contained in a record in this system of records under the routine uses listed in this system of records notice without the consent of the individual if disclosure is compatible with the purposes for which the record was collected. These disclosures may be made on a case-by-case basis, or if the Department has complied with the computer matching requirements of the Privacy Act, under a computer matching agreement. The routine uses are: Program Purposes, Disclosure in the Course of Responding to Breach of Data, Contract Disclosure, Disclosure for Use by Other Law Enforcement Agencies, Enforcement Disclosure, Litigation and Alternative Dispute Resolution (ADR) Disclosure, Disclosure to U. S. Department of Justice (DOJ), Adjudicative Disclosure, Disclosure to Parties, Counsel, Representatives, or Witnesses, Freedom of Information Act (FOIA) and Privacy Act Advice Disclosure, Disclosure to DOJ, and Congressional member Disclosure.
5.7 □ N/A How is the information shared and used by the external entity?

The Department of Treasury uses the information to attempt collection of the scholar debts and to establish wage-garnishment as needed.

5.8 □ N/A Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Please answer YES or NO.

No

5.9 □ N/A Does the project place limitation on re-disclosure? Please answer YES or NO.

No

6. Redress

6.1 □ N/A What are the procedures that allow individuals to access their own information?


4 If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed to Section 7 - Safeguards.
6.2 □ N/A What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Scholars may edit all personal information except for SSN and name. To make edits to these fields, scholars must contact the PDPDCS Help Desk and provide documentation to support the correction. Errors in funding, degrees attained, and service obligation, may be reported by the scholars to the PDPDCS which then communicates with the grantee to determine the correct information.

6.3 □ N/A How does the project notify individuals about the procedures for correcting their information?

Instructions for contacting the PDPDCS Help Desk to correct errors is provided on the scholar's main page.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1 □ N/A Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible? Please answer YES or NO.

Yes
7.2 N/A What procedures or access controls are in place to determine which users may access the information and how does the project determine who has access?

People who have access to the PDPDCS are the grantee project director, a designated secondary user, the scholar, system administrators and PDPDCS Help Desk personnel. ED CORs have "read only" access. A list of all contract personnel and ED staff with administrative access are reviewed and approved annually by the Information System Owner (ISO).

7.3 N/A What administrative, technical, and physical safeguards are in place to protect the information?

The PDPDCS, a secure, online system, has had extensive security testing and meets all security requirements for a moderate level system. The information is secured according to the requirements found in all applicable Department of Education policy and guidance documents. The system complies with IT security requirements in the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circulars, and the National Institute of Standards and Technology (NIST) standards and guidance. The PDPDCS is monitored continuously by the ISO, the Office of Special Education and Rehabilitative Services's (OSERS) Information System Security Officer (ISSO), and by the contractor. Security scans are conducted monthly by the contractor and submitted into CSAM for review by the ISSO and ISO. All vulnerabilities are identified, documented and resolved in accordance with Federal requirements. Privacy risks are ameliorated by careful control of the data. Electronic information is secured through the use of access controls, background clearances, personnel security awareness and training, and regular auditing of information and information management processes. All users are properly identified and authorized for access, are made aware of the rules, and agree to abide by them as stated. In addition, security is maintained through carefully managed control of system changes, appropriate contingency planning, handling, and testing, and by ensuring that any incident is handled expeditiously. Additionally, the system is protected through proper maintenance with controlled regulation of the operating environment and extensive evaluation of information management risks.

7.4 N/A Is an Authority to Operate (ATO) required? Please answer YES or NO.

Yes

7.5 N/A Is the system able to provide account of any disclosures made? Please answer YES or NO.

Yes
7.6 □ N/A Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by federal law and policy? Please answer YES or NO.

Yes

7.7 □ N/A Has a risk assessment been conducted where appropriate security controls to protect against that risk been identified and implemented? Please answer YES or NO.

Yes

7.8 □ N/A Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the controls continue to work properly at safeguarding the information.

The contractor conducts vulnerability scans on a weekly basis and before system changes are released to production. All changes to the web site and database are thoroughly tested in the PDPDCS development and staging environments. All security controls for the PDPDCS are assessed annually by either a Department contractor or through a self-assessment.

8. Auditing and Accountability

8.1 □ N/A How does the system owner ensure that the information is used in accordance with stated practices in this PIA?

The ISO assures that information is used in accordance with Federal regulations and stated practices by monitoring all work associated with the system: security assessments, on-going vulnerability scanning, debt referrals, background clearances at the 5c level for contractor personnel working with the PDPDCS, annual security and role-based trainings, approval of administrative access to the system by contractor personnel and ED staff. Since the ISO is the COR, there is significant oversight across all program offices and activities. The ISO maintains a weekly meeting with program offices to assure ongoing information sharing regarding practices. Further the ISO monitors to assure that encryption is used on all email that contains sensitive information. In a new contract awarded in 2017, the ISO is overseeing the implementation of multi-factor authentication to the PDPDCS.
Privacy risks include the disclosure of SSNs of scholars. To mitigate the risk of disclosure of scholar SSNs, procedures were established to redact the SSN from the Pre-scholarship Agreements prior to their being scanned or uploaded into the PDPDCS. Redacted hard copies of the agreements must be retained by the grantee until the service obligation has been fulfilled. This reduces the risk of disclosure of the SSN due to redaction. SSNs are not stored in the main database, but to mitigate the risk of SSN disclosure, the SSNs are stored in a code in a separate data base and not linked to the scholar. New users are required to access the system through a key code, and then establish their unique password. Passwords expire and must be reset by the user every 90 days. SSNs are only used for debt referral to verify the identity of the scholar. The SSN is not required on any forms except the Pre-Scholarship Agreement. We eliminated the use of SSN on the Exit Certification to mitigate the risk of disclosure of the scholar SSN.