Privacy Impact Assessment (PIA)

for the

Personnel Development Program Data Collection System (PDPDCS)

October 29, 2019

For PIA Certification Updates Only: This PIA was reviewed on **October 29, 2019** by **Richelle Davis** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Richelle Davis
Contact Email: Richelle.Davis@ed.gov

System Owner

Name/Title: Richelle Davis
Principal Office: Office of Special Education Rehabilitative Services (OSERS)

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 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 Division (ARBMD) 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. Describe the purpose for which the personally identifiable information (PII)[1] 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 ARBMD when the scholar's obligation has not been fulfilled through service.

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?

[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

Updated PIA

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 name and citation of the authority.

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. 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

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

18-16-04, Personnel Development Program Data Collection System (PDPDCS), 84 FR 32889-32895, dated July 10, 2019
https://www.federalregister.gov/documents/2019/07/10/2019-14690/privacy-act-of-1974-system-of-records

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

Click here to enter text.

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.

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. Records in system are considered temporary, cut off files annually. Destroy/ Delete 5 years after file cutoff.

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

[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

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.

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

Yes

3.3. What are the sources of PII 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 contact, 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 defined 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.

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

The data are submitted at https://pdp.ed.gov. In rare cases, paper alternative forms may be used.

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?

The information is validated by the grantee who submits a scholar record for each scholar receiving funding; 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. This is a manual process the contractor randomly selects employment records and contacts the employers to verify that the employer actually completed the employment verification and the data are accurate. There are automated validations built into the system, as well, to check for things like internal consistency (that an enrollment date isn't after a date of graduation or the dates aren't in the future), correct formats (e.g., SSN's are 9 digits) and to check for missing required items .

Use

3.6. Describe how the PII is used 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 ARBMD. 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. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

Yes

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

☐ N/A

[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.

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

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.

Yes

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

☐ N/A

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 ARBMD. If a scholar defaults on payment, ARBMD must provide an SSN when referring the debt to the Department of Treasury. Both ARBMD and the Department of Treasury require SSNs to confirm identity and process the debt. There are no alternatives possible for this purpose.

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

☐ N/A

There are no alternatives possible for this purpose.

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.

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. 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

https://pdp.ed.gov/OSEP/home/privacy
https://pdp.ed.gov/OIE/home/privacy
https://pdp.ed.gov/RSA/home/privacy

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?

If scholars 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.*"

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.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

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 ARBMD. 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.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☐ N/A

The purpose of sharing information with ARBMD 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

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.

Yes

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

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 ARBMD 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. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

The purpose for sharing information externally is for when debt is referred to the Department of Treasury for collection.

[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.

5.7. Is the sharing with the external entities authorized?

☐ N/A

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

Yes

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

☐ N/A

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

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

No

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

☐ N/A

No

6. Redress

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

The SORN is located at https://www.federalregister.gov/documents/2019/07/10/2019-14690/privacy-act-of-1974-system-of-records. Scholars may access their own information through the PDPDCS system at any time by using their login information.

6.2. 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. 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. 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 Authority 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?

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.

7.5. 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 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. How does the system owner assess and ensure that the PII 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. Further the ISO monitors to assure that encryption is used on all email that contains sensitive information.

8.2. Does the system owner 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 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. In the fall of 2018, the contractors began introducing Multi-Factor Authentication to users. SSNs are only used for debt referral to verify the identity of the scholar. The SSN is not required on any forms except the PreScholarship Agreement. We eliminated the use of SSN on the Exit Certification to mitigate the risk of disclosure of the scholar SSN.