Privacy Impact Assessment (PIA)

for the

Personnel Development Program Data Collection System (PDPDCS)

May 26, 2021

For PIA Certification Updates Only:

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 (PDP) Data Collection System (PDPDCS) is a public-facing website and web-based data system. The system provides for the collection of data from members of the public, specifically grantees, scholars, and the scholars' employers, for three program offices within the Department of Education (the Department): the Office of Special Education Programs (OSEP); the Rehabilitative Services Administration (RSA); and the Office of Indian Education (OIE). OSEP and RSA are part of the Department's Office of Special Education and Rehabilitative Services; and OIE is part of the Department's Office of Elementary and Secondary Education. All three program offices fund personnel development programs that award grants to Institutions of Higher Education (IHEs) that provide financial support to undergraduate and graduate students. OSEP and RSA refer to the students receiving grant funds as "scholars," while OIE uses the term "participants." For simplicity, this PIA will refer to them all as "scholars." As a condition of receiving grant funds, scholars agree to complete a service obligation. If they are unable to fulfill their service obligation, they must repay the funds to the Department. The purpose of the data collection is to track the enrollment, eligible employment, and service obligation fulfillment of scholars who have received PDP funds, until the scholars' service obligations are fulfilled, or they are referred to the Department's Accounts Receivable and Bank Management Division (ARBMD) within the Office of Finance and Operations (OFO) for repayment of part or all of the funds received.

The specific data collected include the following for each scholar: name, date of birth, Social Security number (SSN), personal mailing address, personal phone numbers, financial account information, personal email address, education records, employment status, and place of employment. This information is provided by the grantee and the scholar. Employers are asked to verify the employment information provided by the scholar. Each program office requires scholars to submit different legal documents related to their ability to accept funding and understanding of the terms of the accepted funding. Each OSEP and RSA scholar completes a Pre-scholarship Agreement (PSA) and Exit Certifications (EC). The PSA notifies the scholar of the program requirements for accepting funds and is signed at the time the scholar enrolls in the grant program by both the grantee and the scholar. The EC provides the final amounts of funding received and total service obligation owed and is signed at the time the scholar exits the grant program by both the grantee and the scholar. OIE scholars complete a Service Payback Agreement (SPA). The SPA is similar to the PSA as it notifies the scholar of the program requirements for accepting funds and is signed at the time of enrollment in the grant program by both the grantee and the scholar. RSA scholars must submit proof of citizenship and complete the certification of eligibility for Federal assistance in certain programs. Subsequent references in this PIA to "legal documents" include all of the documents listed above.

The project director for the grantee registers for an account in the system and is responsible for adding scholar records for the grant. During the registration process, the system collects name, email address, username, and password from project directors. The project director provides the initial scholar information (e.g., SSN, demographics, and contact information) as well as information related to the grant program. Once a grantee submits a record for a scholar, the scholar is sent an automated invitation email providing them with instructions on how to log into the system. The grantee reports the enrollment status of the scholar at the end of each academic year (e.g., the scholar is still enrolled in the grant program; the scholar has completed the grant program; or the scholar has exited the grant program prior to completion).

If and when a scholar submits employment information, the PDPDCS emails the scholar's employer to verify the information. Employers are prompted via email to access the site and verify scholar employment. Scholars receive credit toward their service obligation for verified employment.

The PDPDCS also provides technical assistance to all users and generates performance data for reporting annually on program results.

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

Information about scholars 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.

Information is collected from grant project directors so they can register for an account in the system and add scholar records for the grant. The project director also provides the initial scholar information (e.g., SSN, demographics, and contact information) as well as information related to the grant program and the status of the scholar at the end of each academic year.

Information is collected from contractors so they may access the system for administrative purposes.

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

This PIA is being updated as part of the regular 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 name and citation of the authority.

All three program offices are required under The Government Performance and Results Act of 1993 (GPRA), Public Law103-62, to collect and report program performance measures. The PDPDCS is the primary source of data for all three programs' performance measures. In addition, each personnel training program is funded under a specific law and is regulated under individual regulations.

For OSEP, the Individuals with Disabilities Education Improvement Act (IDEA), Public Law 108-446 addresses providing personnel development to improve services and results for children with disabilities. The program requirements regarding service obligations are specified in Service Obligations Under Special Education - Personnel Development to Improve Services and Results for Children with Disabilities, 34 C.F.R. § 304 (2006).

For OIE, the Elementary and Secondary Education Act (ESEA), reauthorized by Congress at the end of 2015 as the Every Student Succeeds Act (ESSA) (P.L.114-95), provides funding for professional development for teachers and educational professionals to improve outcomes for Indian children. Under section 6122(h) of the ESEA, the Secretary must require, by regulation, that individuals who receive training under this program either perform work related to the training and that benefits Indian students in a local educational agency that serves a high proportion of Indian students or repay all or a prorated part of the assistance received. Under the program regulations implementing this requirement, when participants graduate from their pre-service training program, they must report on their employment status every six months. 34 CFR 263.10(b).

For RSA, 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. The program regulations, 34 CFR 386, CFR 367 et.

seq., provide further specificity regarding the service obligation requirements.

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

18–04–04, Education's Central Automated Processing System (EDCAPS); 80 FR 80331- 80339, dated December 24, 2015. https://www.federalregister.gov/documents/2015/12/24/2015-32501/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

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.

Information collected from scholars includes: name, date of birth, SSN, personal mailing address, personal phone numbers, financial account information, legal documents, personal email address, education records, employment status, and place of employment.

Information collected from grantee program directors includes: name, email address, name of institution, title, phone number, username, and password.

Information collected from contractors accessing the system for administrative purposes includes: username, email address, and password.

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

Yes

The scholar PII collected is the minimum needed to track their enrollment and service obligation fulfillment and to refer scholar debt to ARBMD when the scholar's obligation has not been fulfilled through service.

Only name and email address are collected from grantee program directors so they can register for an account to discharge their responsibilities.

Information is collected from contractors so they may access the system for administrative purposes.

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 applicable 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 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 through online web forms at https://pdp.ed.gov. In rare cases, paper alternative forms maybe used.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected? 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 through which 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 forthings like internal consistency (that an enrollment date is not after a date of graduation orthe dates are not in the future), correct formats (e.g., SSNs are nine 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 are used in conjunction with data collected by the PDPDCS to calculate results for program performance measures. Information from the Department’s grants database, G5, 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?

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.

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 for repayment to ARBMD. If a scholar defaults on payment, ARBMD must provide an SSN when referring the debt to the U.S. Department ofthe Treasury. Both ARBMD and the U.S. Department of the 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.

The Privacy Act Statement is included on the PSA and EC for OSEP and the SPA for OIE. RSA is in the process of creating standardized PSAs and ECs and will include the language. Users must acknowledge the Privacy Act Statement after logging into the PDPDCS. The statement is presented as a pop-up message that must be accepted. A SORN for the PDPDCS is available at https://www.federalregister.gov/documents/2019/07/10/2019-14690/privacy-act-of-1974-system-of-records.

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

OIE SPA: https://pdp.ed.gov/OIE/Content/pdf/1810-0698%20PD_payback_agreement-120120.pdf

OSEP PSA: https://pdp.ed.gov/OSEP/Content/pdf/1820-0686_Pre-Scholarship_Agreement%20OPP%2008-31-23.doc

OSEP EC: https://pdp.ed.gov/OSEP/Content/pdf/1820-0686_Exit_Certification%20OPP%2008-31-23_new.doc

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 PSA or SPA, scholars opt out of the program.

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 that 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 aggregated 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 programevaluation data sharing. Data compiled without PII may also be shared with Department 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 Department 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

If a scholar elects to enter cash repayment or is required to enter cash repayment per program regulations, PDPDCS provides ARBMD with the scholars' information, including SSN. This disclosure of information is covered as a routine use under the EDCAPS SORN. ARBMD is responsible for collecting funds from scholar and has contracted with Centralized Receivables Service (CRS) to accomplish this task. Should the scholar default on a repayment plan or be non-responsive to the Department'srequest for repayment, scholar information, including SSN, is forwarded by ARBMD to the U.S. Department of the Treasury for collection.

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

□ N/A

The information is shared with the Department of Treasury for collection of the money owed.

The PDPDCS itself does not currently share data externally with non-Federal entities, and would only do so for a legitimate, authorized purpose, as permitted by a routine use, consent of other Privacy Act exception.

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 information is shared via encrypted email.

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?

Yes

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 procedures for accessing information are described in the SORN, which 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 informationthrough 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 policy. The system complies with IT security requirements in the Federal Information Security Modernization Act (FISMA), Office of Management and Budget (OMB) circulars, and the National Institute of Standards and Technology (NIST) standards and guidelines. The PDPDCS is monitored continuously by the Information System Owner (ISO), the Office of Special Education and Rehabilitative Services' (OSERS) Information System Security Officer (ISSO), and by the contractor. Security scans are conducted monthly by the contractor and reviewed 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, appropriatecontingency planning, handling, and testing, and by ensuring that any incident is handledexpeditiously. 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 Department staff. Since the ISO is the Contracting Officer’s Representative (COR), there is significant oversight across all program offices and activities. Further the ISO monitors to assure that encryption is used on allemail that contains PII or 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?

The ISO ensures the information is used in accordance with stated practices by confirming the privacy risks are properly assessed, ensuring Privacy Act records are maintained in accordance with the provisions of the Federal Records Act, Departmental policies, the Privacy Act, and the published SORN, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. The ISO participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in the Office of the Chief Information Officer's Lifecycle Management Methodology (LMM), which addresses security and privacy risks throughout the systems' life cycle. In addition, PDPDCS has established procedures to redact SSNs from PSAs, SPAs, and ECs. SSNs are encrypted in the PDPDCS database. 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. MFA is required for all administrative users, grantees, and RSA scholars. OIE and OSEP scholars will be required to use MFA in the fall of 2021.