Privacy Impact Assessment (PIA)

for the

Perkins Information Management System (PIMS)

November 24, 2021

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Jose Figueroa
Contact Email: Jose.Figueroa@ed.gov

System Owner

Name/Title: Denise Dupont
Principal Office: OCTAE

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 Division of Academic and Technical Education (DATE), within the Office of Career, Technical, and Adult Education (OCTAE) manages an investment called the National Perkins Information System (NPRS) contract. This investment is comprised of two projects: the Perkins Information Management System (PIMS) and the Perkins Collaborative Resource Network (PCRN).

PIMS contains a variety of databases, such as the Consolidated Annual Report (CAR) Database, State Plan Submission Database, Monitoring Database, and PIMS Contact Database. PIMS supports DATE's program administration and accountability efforts by maintaining and operating existing databases (PIMS) and a public website (PCRN), ensuring the validity and reliability of data contained therein.

Pursuant to 20 U.S.C. § 2323, 2 CFR § 200.327, and 34 CFR § 76.720, each eligible agency that receives an allotment under 20 U.S.C. § 111 shall annually prepare and submit a report to the Secretary of Education (Secretary). The purpose of the CAR is to be a repository for these statutory and regulatory federal reporting compliance elements.

The CAR database collects the following elements:

- Narrative performance reports
- Financial reports
- State-level aggregate career and technical education student enrollment and performance reports

Pursuant to 20 U.S.C. § 2342, each eligible agency desiring assistance for career and technical education for any fiscal year shall prepare and submit to the Secretary a State plan for a 4-year period. The State Plan Submission database was designed to be a repository for this requirement.

The State Plan Submission Database collects the following information:

- A cover page, including a letter providing joint signature authority from

State officials
- Narrative descriptions of the state plan
- Assurances, certifications, and other forms required by statute and/or applicable Federal regulations, including Education Department General Administrative Regulations (EDGAR)
- Budget for upcoming year
- State aggregate student performance data

The Monitoring Database tracks and archives DATE's State risk analysis, monitoring reports, and pass-through entity requirements[1].

The PIMS Contact Database is used to archive the names, job titles, email addresses, and phone numbers of State and Federal employees who request login credentials for PIMS. Contact information is collected via email from State officials prior to creating their accounts. State agency directors are contacted annually and following staffing changes; these officials send the required information to the program office via email. Login credentials (username and password) are also stored in the system. This information is only available to DATE management and staff.

Every year, DATE collects State aggregate student performance data, fiscal reports, and narrative elements from its grantees, which are submitted via a secure portal within the PIMS and restricted to State career and technical education (CTE) staff who have been given access to the system for their particular State. In addition, information in PIMS is restricted to DATE staff and managers within OCTAE who manage Perkins formula grants. Access to PIMS is restricted according to an individual's role and responsibilities. There are three levels of access to PIMS:

- **Level One** access is restricted to external users such as State Directors, State fiscal auditors, and State performance Directors, who are required to access the system in order to submit and certify their CAR reports and State plans. Level One access is only provided to State CTE Directors, State fiscal auditors, and State performance data Directors. These external users are certified by the State CTE. DATE collects the name, official title, and email of the people who will have access to the system. External users do not have access to the internal databases contained within PIMS, nor do they have access to our contact list of State users.
- **Level Two** access is granted to staff within DATE, based on their job description and duties as grant managers. These grant managers are restricted access to only those States under their supervision.

[1] For additional information on these requirements, please refer to the following resource: 2 CFR § 200.332 - Requirements for pass-through entities. | CFR | US Law | LII / Legal Information Institute (cornell.edu)

- **Level Three** access is granted to a limited number of PIMS database administrators, the Division Director, Branch Chief, and the project manager within DATE, all of whom oversee the operation and management of PIMS.

Information submitted by the State is certified by the State CTE director and/or financial officer via electronic signature and passcode. The CAR and State Plan Submission databases are used by State CTE directors to submit required annual documentation. The information that is submitted by the State is comprised of narrative explanations of how the State intends to implement its Perkins program throughout the State; as well as the proposed annual budget for the following fiscal year. The State plan does not collect any PII with the exception of the name, email, and address of the State CTE Director; which is public information.

PCRN is a publicly accessible website that serves as the main website for DATE. PCRN disseminates program information to grantees and is used by State CTE directors, teachers, students, parents, researchers, and other stakeholders. The website contains general information regarding grants, DATE activities, learning resources, reports to Congress, and State-level aggregate, deidentified student data. The PCRN website does not collect any information. The website is intended to provide information to the general public regarding the career and technical education, program memoranda, and technical assistance resources. Neither PIMS nor PCRN contains student, district, or school-level data; all data in the systems are aggregate and deidentified.

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

PII is collected by the system to create login credentials for user accounts and to facilitate the Department's authorization of the state's data quality certification and financial report.

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?

New PIA

This is a new PIA because during the bi-annual review, it was determined that a PIA is required when previously it was determined to not be required.

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.

Authorized under section 114 (c) (1) of the Strengthening Career and Technical Education Act for the 21st Century Act (Perkins V).

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?

No

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

Click here to enter text.

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

Information is not retrieved by name or other personal identifier.

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.

Records created and received by PIMS will not be destroyed until an appropriate Departmental records disposition schedule is developed and approved by the National Archives and Records Administration (NARA). The Department's Records Officer is currently processing changes to records retention schedules, which will impact PIMS.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Records are not currently being disposed of since the Department's Records Officer is currently processing changes to records retention schedules, which will impact PIMS.

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.

The PIMS Contacts Database: name, job title, work email address, and work phone number of state and federal government employees who request login credentials to use the system. Login credentials (username and encrypted password) are also stored in the system.

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

Yes

The system collects the minimum amount of information for the creation of account for access to the system.

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

PII is collected directly from Federal employees. State agency officials provide state user information to DATE staff.

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 name and work contact information are collected via email from the state agency

officials prior to creating the user account. DATE staff contact the state agency directors annually and following staffing changes, and these officials send the required information to the program office. The state agency program director or other authorized state agency leadership must send the prospective state user's name and work contact information; information received directly from prospective users is not accepted. DATE staff create user accounts for the State officials.

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 PII collected (name, work email address, and work phone) is validated and confirmed to ensure the integrity of the information collected. We do this by contacting the state director each time we receive notice of state employee staffing changes and for all state staff at least annually.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

State and Federal government employees' names, email addresses, and phone numbers are collected to provide contact information for establishing user credentials and facilitate the certification process. To certify and submit the application, the state employee must enter their username and password to verify their identity. The system populates this information into the form.

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

Click here to enter text.

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.

No

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

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

4. Notice

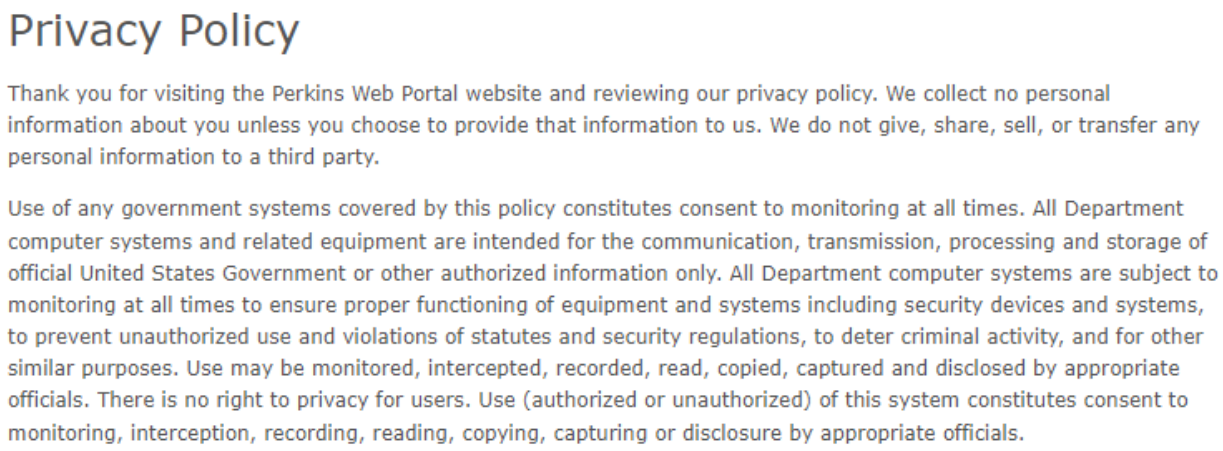
4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA,)? If notice is not provided, explain why not.

Notice about the collection of PII is provided prior to the creation of state and federal employee user accounts at the time they are requested by state and federal agency officials. In addition, the link to the PCRN privacy policy is displayed on our site at cte.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

The text is below:



Privacy Policy

Thank you for visiting the Perkins Web Portal website and reviewing our privacy policy. We collect no personal information about you unless you choose to provide that information to us. We do not give, share, sell, or transfer any personal information to a third party.

Use of any government systems covered by this policy constitutes consent to monitoring at all times. All Department computer systems and related equipment are intended for the communication, transmission, processing and storage of official United States Government or other authorized information only. All Department computer systems are subject to monitoring at all times to ensure proper functioning of equipment and systems including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for other similar purposes. Use may be monitored, intercepted, recorded, read, copied, captured and disclosed by appropriate officials. There is no right to privacy for users. Use (authorized or unauthorized) of this system constitutes consent to monitoring, interception, recording, reading, copying, capturing or disclosure by appropriate officials.

The PCRN Privacy Policy providing notice can be found here: PCRN: Privacy Policy (ed.gov)

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?

State and federal employees who want to access the system must submit their name and contact information through the system to obtain login credentials and a confirmation number required to certify the submission.

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.

No

5.2. What PII will be shared and with whom?

☑ N/A

Click here to enter text.

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

☑ N/A

Click here to enter text.

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.

No

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

Click here to enter text.

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

☑ N/A

5.7. Is the sharing with the external entities authorized?

☑ N/A

Click here to select.

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☑ N/A

Click here to select.

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

☑ N/A

Click here to enter text.

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

Click here to select.

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

☑ N/A

Click here to select.

6. Redress

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

Each federal and state employee has a user account to access or update their own information through My Accounts page in PIMS.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If individual user information has changed or is inaccurate, the federal or state employee can update the information themselves or request assistance by sending an email message to cte@ed.gov.

6.3. How does the project notify individuals about the procedures for correcting their information?

The project uses webinars, email, memos, and individual technical assistance to notify individuals about the procedures for correcting their information.

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

Low

7.4. What administrative, technical, and physical safeguards are in place to protect the

information?

Access to the system is only available to authorized users with login credentials. User access is managed by the DATE program office. DATE has technical and administrative controls inplace that are compliant with the Federal Information Security Modernization Act (FISMA) and with National Institute of Standards and Technology (NIST) standards and guidelines.

The system also operates under an approved Authorization to Operate (ATO). The System Security Plan details the security and privacy requirements and describes the controls that are in placeto meet those requirements. The system offers a high degree of resistance to tampering and circumvention. This security system limits data access to Department and contract staff on a "need to know" basis and controls individual users' ability to access and alter records within the system.

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 project's technical team lead, OCTAE's IT specialist, monitors security controls at least on a weekly basis. While OCTAE has purview over the application's security controls,it does not have control over the security controls in the hosting environment managed by the contractor. The contractor regularly monitors the security controls for the hosting environment.

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 system owner ensures that the information is used in accordance with stated practices in this PIA through several methods. One method is completing the ED Risk Management Framework process and receiving an Authority to Operate (ATO). Under this process a variety of controls are assessed by an independent assessor to ensure the system and the

data residing within are appropriately secured and protected. The PIA is reviewed and updated on an as-needed basis and at a minimum, every two years. These methods together with regular communication with the NPRS users ensures that the information is used within the stated practices outlined in this PIA.

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?

This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data from privacy threats and mitigate the risks to the data. One key risk to the data is unauthorized access to the PII. The risks are mitigated by the above-mentioned controls and safeguards. Additional privacy risks are mitigated as the system collects the minimum necessary PII to achieve the purpose and the information collected is considered to be fairly low risk, as it is only name and work contact information and does not include any elements that have been identified as sensitive.