Privacy Impact Assessment (PIA)
for the

National Reporting System - Database
February 26, 2021

For PIA Certification Updates Only: This PIA was reviewed on 3/2/2021 by Michael V Feranda certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Michael V Feranda
Contact Email: Michael.Feranda@ed.gov

System Owner

Name/Title: Michael V Feranda
Principal Office: Office of Career, Technical, and Adult Education (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 National Reporting System (NRS) for Adult Education Reporting Database (NRS RPT DB) is the accountability data collection application for the federally funded adult education program, authorized by Section 212 of the Adult Education and Family Literacy Act (AEFLA). Section 212 of AEFLA requires that the Department of Education's (Department) programs and activities authorized under AEFLA are subject to the performance accountability provisions described in Section 116 of the Workforce Innovation and Opportunity Act (WIOA). The purpose of Section 116 in WIOA is to establish performance accountability measures that apply across the core programs to assess the effectiveness of states in achieving positive outcomes for individuals served by those programs.

NRS RPT DB is the required comprehensive performance accountability system established for formula grantees to assess the effectiveness of adult education and literacy activities authorized under AEFLA. The NRS RPT DB annually collects and stores aggregated state-level program performance data. The state reports program outcomes for the entire state on a state-level table. While the state collects individual participant data, it does not report individual record data to us. For example, the state reports employment rates or measurable skill gain rates for an entire group of program participants.

The NRS RPT DB system is hosted on an ETS and IBM SmartCloud dedicated government service hosting environment. NRS RPT DB is a FIPS 199 low-impact, minor application that provides a front-end website and back-end database. NRS RPT DB also contains login information using state/federal employee name and employee email information. Phone numbers are optional but not normally collected for the application. Private citizens are not authorized to obtain NRS RPT DB accounts and all authorized users are required to use public state/federal contact information.

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 electronic signature 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

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 by Section 212 of the Adult Education and Family Literacy Act (AEFLA).

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?

[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

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.

GRS 5.2 Transitory and Intermediary Records
Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

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

[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

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.

Name, job title, work email address, and work phone number of state and federal government employees who request login credentials to use the system for reporting. 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 information is needed to provide federal and state employees with login credentials and to facilitate electronic signatures. No additional information is collected.

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

State and federal government employees.

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 is collected via email from the state agency officials prior to creating the user account. State agency directors are contacted 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.

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?

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 electronic signatures. Electronic signatures (which consist of state employee name, email address, phone number, and job title) are maintained in this system. To provide an electronic signature, the state employee must enter their username and password to verify their identity and have the system populate 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 ED.gov privacy policy is displayed on our site at https://nrs.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 Department web policy providing notice can be found here:
https://www2.ed.gov/notices/privacy/index.html

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 to obtain login credentials and the ability to electronically sign a document.

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

Click here to enter text.

5.7. Is the sharing with the external entities authorized?

☑ N/A

[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.

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.

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 NRS@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 NRS program office. NRS has technical and administrative controls in place 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. The System Security Plan details the security and privacy requirements and describes the controls that are in place to 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 leader, OCTAE's IT specialist, monitors security controls on at least 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 Pivot contractor. The contractor is expected to regularly monitor 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 NRS 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.