Privacy Impact Assessment (PIA)

for the

National Reporting System Website for Technical Assistance (NRS WEB TA)

July 18, 2022

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: Mike Feranda/IT Specialist
Contact Email: michael.feranda@ed.gov

System Owner

Name/Title: Michael Feranda/IT Specialist
Principal Office: Office of Career, Technical, and Adult Education

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) Website for Technical Assistance (NRS WEB TA) is a technical assistance website and documentation repository for State-administered, Federally funded adult education activities which are conducted under the Adult Education and Family Literacy Act (AEFLA). Developed by the U.S. Department of Education (Department) Office of Career, Technical, and Adult Education's (OCTAE) Division of Adult Education and Literacy (DAEL), the NRS continues a cooperative process through which State adult education directors and DAEL staff manage an accountability system that documents program outcomes for adult education. NRS WEB TA provides the following features to support the mission of the adult education program:

- A web-based platform used as a central repository for uploading and storing technical assistance documentation.
- An NRS Moodle site that provides access to online courses for State and local adult education staff. Because it is not always possible to attend training in-person, DAEL has developed online courses that adult education staff can access to learn about NRS requirements and acquire strategies for improving NRS data quality.

To access online courses, State and local adult education staff must create accounts within the system. Users access the system via username and password. The following information is collected during account creation: name, email address, city/town, and State/Territory in which adult education program is located. The site tracks users' course progress and enables users to continue courses from where they left off.

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

[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

PII that is collected and maintained within NRS WEB TA is used to establish and maintain user accounts for State and local adult education staff. Specifically, city/town and State/Territory in which the adult education program is located are collected to determine and track which program in each city, town and State the Department has assisted. Accounts are used to access online training courses maintained by the system and track user progress.

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 a regular biennial review.

1.5. Is the system operated by the agency or by a contractor?

Contractor

The NRS WEB TA is administered by the American Institutes for Research (AIR).

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.

The authority for collecting, maintaining, and using information about the public for the purpose identified in Question 1.2 is the Adult Education and Family Literacy Act (AEFLA) Section 212 (90 U.S.C. § 9212).

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

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

OCTAE does not retrieve information from the system by a unique 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.

In accordance with GRS 5.2 Transitory and Intermediary Records, records are considered temporary and should be destroyed 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

[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.

First name, last name, email address, city/town, username, password, and the State/Territory in which the adult education program is located.

All fields are required except for city/town.

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

Yes

The PII collected and maintained is the minimum amount required by NRS WEB TA to establish user accounts for the purpose of accessing specific training resources. Specifically, city/town and State/Territory in which the adult education program is located are collected to determine and track which program in each city, town and State the Department has assisted. No additional information is collected.

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

NRS WEB TA collects information from State government staff and local adult education staff who register for an account to access the training.

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

User registration can either be initiated by the individual users or by the site administrator in response to a request from State government and local adult education staff. Users can create their own accounts to self-register for online courses. If a user is having technical issues with registration, users can send the information needed to create an account by email directly to the administrator or project staff. A password is assigned for initial login and must be updated by the users upon first login.

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?

When a user creates a new account via self-registration, the system sends an email to the user and asks them to confirm their account. Once the account is confirmed, there is no further validation.

Use

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

PII that is collected and maintained within NRS WEB TA is used to establish user accounts for State and local adult education staff. User accounts are used to access online training courses maintained by the system. The site also tracks users' course progress and enables users to continue courses from where they left off.

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.

No

[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.

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

☑ N/A

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

☑ N/A

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, etc.)? If notice is not provided, explain why not.

The system provides a privacy notice whenever users create an account or log in to the system.

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 privacy notice is located on the NRS WEB TA login webpage.

Authorities: The following authorizes the collection of this information: Adult Education and Family Literacy Act (AEFLA) Section 212 (90 U.S.C. § 9212).

Information Collected: first name*, last name*, email address*, city/town, username*, password*, and the State/Territory in which the adult education program is located*.

NOTE: * denotes required fields.

Purpose: The purpose of collecting this information is to establish user accounts for State and local adult education staff, which are used to access online training courses maintained by the system.

Disclosures: The information will not be disclosed outside of the Office of Career, Technical, and Adult Education.

Consequences of Failure to Provide information: Failure to provide required information or forego creating an account may result in not gaining access to the courses maintained on the system.

Additional information about this system can be found in the Privacy Impact Assessment.

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?

Individuals can choose to not provide information to create an account but doing so will prevent access to the courses maintained on the system.

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

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

☑ N/A

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

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

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?

[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.

System users can log into NRS WEB TA using their credentials and access their own information within the system.

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

Users can email the website administrator to correct their information. Users who forget their password or want to change it can click on the "forgot password" link on the NRS WEB TA login webpage and enter their email or username. The system sends an email to the user to reset their password.

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

The user is informed to email technical support for assistance or if help is needed in correcting information. To change the password, the user can click on the "forgot password" link on the NRS WEB TA login webpage and enter their email or username. The system sends an email to the user to reset their password.

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 Authorization 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?

NRS WEB TA is maintained on secure computer servers located in one or more secure contractor network server facilities. Administrative access to NRS WEB TA is limited to authorized contractors and Department employees. In accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Office of Management and Budget (OMB) policy, NRS WEB TA must receive a signed ATO from a designated Department authorizing official. Security and privacy controls implemented by NRS WEB TA are comprised of a combination of administrative, physical, and technical controls.

All users accessing the system are given unique user identification. The Department requires the enforcement of a complex password policy and two-factor authentication for Department and contract users. In addition to the enforcement of the two-factor authentication and complex password policy, Department and contact users are required to change their password at least every 90 days in accordance with the Department's information technology standards. Physical security of electronic data is maintained in a secured data center, access to which is controlled by multiple access controls. Cryptographic solutions are in place to prevent unauthorized disclosure of information and to protect the integrity of data at rest and in transmission.

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.

AIR performs continuous monitoring of system and web application vulnerabilities and threat information to reduce the likelihood of unauthorized access to PII. Vulnerability and threat information is reviewed weekly as part of a formalized weekly process involving IT, development, and information security staff. Threat information and security logs are monitored 24/7 by trained security operations staff.

AIR conducts the periodic testing and assessments that are appliable to this system. These assessments include: assessments of applicable NIST controls in the system

security plan (SSP), weekly vulnerability scans, monthly web application and database vulnerability scans, incident response and contingency plan testing, and annual penetration testing.

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 works with the Department's Privacy Program to complete a PIA and to ensure the PIA is accurate and updated as required. The system owner also completes the Department Risk Management Framework (RMF) process to secure an 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 system owner works with contractors to ensure the system is being used appropriately and in accordance with the practices detailed in this document. These methods along with regular communication with NRS users ensure 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?

Privacy risks associated with NRS WEB TA include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include embarrassment or loss of credentials that are used to gain access to other resources. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Continuous security monitoring of system logs, malware prevention, availability and system health analysis through Azure Sentinel, and monitoring by a 24/7 Security Operations Center (SOC)
- Weekly monitoring of security controls

- Monthly web application, database, and vulnerability scanning
- Annual contingency plan test
- Annual or ongoing security assessments
- Annual cybersecurity and privacy training for Department users

Risks are also mitigated by updating security patches and updating devices' operating software. Scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.