Privacy Impact Assessment (PIA)

for the

Results

April 20, 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: Benjamin Starr, Alternate Information System Owner
Contact Email: Benjamin.starr@ed.gov

System Owner

Name/Title: Patricia Meyertholen, Information System Owner, Migrant Education Programs (MEP) Group Leader
Principal Office: Office of Elementary and Secondary 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.

Results is a website that aims to help coordinate the dissemination of information and guidance from the U.S. Department of Education (Department) Office of Elementary and Secondary Education's (OESE) Office of Migrant Education (OME) to the directors and other members of State Migrant Education Programs (MEP). The Results website contains two elements – a website that provides information to the public, and a Community of Practice (CoP) website that is only accessible by those who are approved by OME for access.

Public Website
On the public website, Results provides general information about migrant education programs, and maintains a directory of State migrant education employees (https://results.ed.gov/resources/state_program_information). The information shown includes migrant education employee name, title, work email, work phone, and work fax number.

Community of Practice (CoP)
In September 2021, Results was updated to include a CoP area of the website. The CoP is a social networking-type application where members of the CoP are associated with affinity groups and are able to make wall posts, leave replies on other wall posts, and share resources. To help coordinate discussions, time-bound learning cycles are held within the CoP. Each learning cycle lasts a few months and has a unique set of participants and a unique content focus. These learning cycles help focus activities on the platform around specific topics. Depending on the learning cycle, there may be one or more subject matter experts invited to help guide and participate in the community. Registration to the CoP is not open to the public. OME requests nominations for participants from State migrant education programs, then reaches out to nominees via email. Those that wish to participate in the CoP confirm with OME and request the learning cycles they would like to participate in. When requesting a CoP account, users provide name, email address, and State. OME then provides the contractor that manages the website with a list of approved participants. The contractor creates accounts for

approved users and groups them into the proper learning cycles and provides technical support for accessing the CoP platform.

The CoP requires authentication using email address and password, and also requires all users to set up and use multi-factor authentication (MFA). The options for MFA include having the code sent to the work email address or users may opt to use an authenticator application such as Google Authenticator.

Once authenticated in the CoP, members can see the first name, last name, associated State, and profile pictures of other participants in the CoP, along with any content posted. Profile pictures are optional. Email addresses are not shared within the CoP.

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

Results utilizes PII to provide a directory of contacts to the public. This allows the opportunity for the public to identify State directors for migrant education and their contact information. This information includes names, titles, work addresses, work email addresses, and phone numbers.

For the CoP, PII is collected to establish accounts for individuals nominated to participate in the CoP. Names and work email addresses are used to identify the CoP participant providing content within the CoP. Posts and resources uploaded to the platform are associated with a user account.

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

During a review of Results, it was determined a PIA is required for this system.

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

[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

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.

Results is authorized by Section 1308 of Title I, Part C, of the Elementary and Secondary Education Act (ESEA), as amended, authorizes the Secretary of Education to set aside a portion of program funds to be used—through grants or contracts with State education agencies, local education agencies, institutions of higher learning, and other public and private nonprofit entities—to improve the interstate and intrastate coordination of migrant education activities. In particular, section 1308(c) authorizes the Department to reserve funds appropriated for the Title I, Part C, Migrant Education Program for the purpose of carrying out the activities described in sections 1308(a)—improvement of interstate and intrastate coordination, 1308(b)—electronic transfer of migrant student records, and 1308(d)—consortium incentive grants.

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] 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

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

Results does not retrieve information by a unique identifier. Information is collected and used to establish user accounts and to post contact information to the public-facing website.

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.

OESE is waiting on the 21st Century Information Retention Policy framework to be approved and implemented. In that framework, OESE results.ed.gov website would fall under DAA-0441-2022-0001-0005 III.A., Department Engagement Program Records.

Until that framework is implemented, the records will not be destroyed until such time as NARA approves said schedule.

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.

- **From users, including Federal employees and contractors, accessing the CoP**:
  - Name

- Work email address
- State
- Password
- Profile picture (optional)
- Any content posted in the CoP by users

- **From State government employees that have contact information posted on the Results website:**
  - Name
  - Title
  - Work email address
  - Work phone number
  - Work fax number

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 Results. Results utilizes PII to provide a directory of contacts to the public. This allows the opportunity for the public to identify State directors for migrant education and their contact information. This information includes names, titles, work addresses, work email addresses, and phone numbers.

For the CoP, PII is collected to vet individuals for access, establish accounts for individuals nominated to participate in the CoP. Names and work email addresses are used to identify the CoP participant providing content within the CoP. Posts and resources uploaded to the platform are associated with a user account.

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

Sources of the PII include: the Department OME staff, State MEP program representatives, and individuals who are approved for access to the CoP.

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

For CoP users, prospective participants email OME to request access to the platform. Their names, email addresses, and associated State are then submitted as a work request to the contractor and an account is generated for the individual.

For contact information for state MEP programs listed on Results, OME informs the contractor of updates to the State Profile pages as they learn of transitions into and out of roles and then submit work requests to have the content updated on the website.

OME has program officers that work with all of the States. When the program officers learn of a new State contact, then the new State contact is asked to provide their contact information and they are notified that the information will be posted on Results. OME also emails the contractor to remove the previous contact's information and add the incoming person's information.

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?

Contact information updates are reviewed as part of a quality control process before the changes are approved by OME for publishing to the production website. Results has a defined Quality Management Plan with many different components. As defined in the plan, when we learn of an updated State contact, OME submits a work request. The contractor receives notification of the request and implements the contact update within the Results website. This update is then posted to a development site where it is reviewed by a second person, comparing the development site content against the work request. If that check is passed, then OME is notified to review and approve the change on the development site. Upon OME approval, the change is then deployed to the production website.

For the CoP, the only requirement is a unique email address to access the system. This is enforced using a number of different software validations. The validity of the email addresses is checked when automated messages are sent from the system. If an email address is incorrect or no longer exists, a bounce record is generated and then reviewed by the contractor. When the bounce is received, the email response is reviewed and if it is no longer a valid email address, the account is disabled within the CoP.

Use

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

[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.

Results is an interstate coordination website and hosts a contact list of MEP State Directors to allow the public to easily find and contact the appropriate MEP representative for their geographic region.

For the CoP, work email address is used to authenticate the platform user, establish an account, and is also used to notify the user of platform activity. Individual names are used within the CoP to help identify the posts, replies, likes, and resources submitted by platform participants.

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

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

The public website includes a published privacy policy that covers the collection of information for the purposes of publishing State directors for migrant education and their contact information for public consumption and for the uses of the CoP.

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 policy can be located at: https://results.ed.gov/pages/privacy_policy.

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?

All the PII associated with Results is volunteered by individuals (OME and State contacts). They may opt out or decline to provide PII. The procedure to remove someone from the directory of State migrant education employees or the CoP is they would contact the Department to request deletion of their information or account.

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

[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.

5.11. 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?

State MEP directors that are listed in the various contact lists on the Results website can review their information for accuracy at any time. Individuals participating in the CoP are able to navigate the platform to find all of the data they have submitted on the CoP.

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

For incorrect contact information, individuals can reach out to OME or submit a request through a distribution email to the contractor (results-info@rti.org). All requests via the email are shared with OME and then a work request is generated to resolve the inaccurate or erroneous information.

For the CoP, users have the ability to delete any data they have uploaded to the platform.

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

A contact email address is featured in numerous places on the Results website and CoP platform. OME contact information is also listed on the Results website. The email address is listed as "Feedback" links present in the header and footer of every page on Results. Additionally, on the State Profiles page, there is a message[5] that references the email address.

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?

[5] "For more detailed information, visit the State's website. To provide updated State Program contact information, please contact results-info@rti.org."

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?

Results is hosted on a secure infrastructure that is FedRAMP-compliant and Department-authorized and is managed using a software development life cycle methodology that includes information security considerations, following an agile, iterative development model. Results meets the current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 security and privacy controls for low systems and was assessed through the formal ATO process.

Results conducts user account reviews on a quarterly basis, reviewing user access granted within the information system. User access reviews help to identify, including but not limited to:

- A terminated employee gaining remote access to the network or email system.
- Segregation of duties issues.
- Misuse of dormant administrative accounts that are still active.
- System compromise using vendor passwords.

The CoP requires an up-to-date operating system on the device that it is accessed from and has strong password and log-in requirements including two-factor authentication. All data are encrypted.

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.

As part of the ATO process, a Department-approved third-party assessor performs an assessment of the Results security and privacy controls. Plans of Actions and Milestones are developed and implemented to ensure that all identified deficiencies are remediated. Results is enrolled in the Ongoing Security Assessment program where the security and privacy controls are tested and evaluated on a quarterly basis to ensure that the controls are working as intended. Additionally, Results is scanned regularly using automated tools to detect vulnerabilities. The results of the vulnerability scans are reviewed and addressed at the application and infrastructure levels.

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 maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, the Results system owner makes sure that the NIST SP 800-53 controls are implemented. The NIST controls comprise of an administrative, technical, and physical controls to ensure that information is used in accordance with approved practices.

The second method is by ensuring that the system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO to ensure the Results system owner or authorized delegate completes reviews of system accounts to ensure only authorized individuals have access to system data.

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 Results include unencrypted data being lost, stolen, or compromised or the potential unauthorized access to the PII contained within the system. Data breaches involving PII are potentially hazardous to both individuals and organizations. Individual harm may include compromise of credentials or embarrassment. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

Results has several privacy risk mitigation strategies in place. The risks are mitigated by granting access to only authorized individuals based on their respective position and on a need-to-know basis, limiting users to those who are screened, utilizing least privilege principles, and encrypting data in transmission. Risks are also mitigated by updating security patches per the patch scheduling and updating devices operating software, amongst other software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. In addition, privacy training is provided for both contractor(s) and Department staff.