Privacy Impact Assessment (PIA)
for the

**WIOA State Plan Portal**

**January 14, 2020**

**For PIA Certification Updates Only:** This PIA was reviewed on January 14, 2020 by Mary Jo Maralit certifying the information contained here is valid and up to date.

**Contact Point**

**Contact Person/Title:** Mary Jo Maralit  
**Contact Email:** maryjo.maralit@ed.gov

**System Owner**

**Name/Title:** Mary Jo Maralit  
**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.

Under the Workforce Innovation and Opportunity Act (WIOA), States are required to submit State Plans to the Secretary of Labor at the Department of Labor (DOL). The State Plans are shared with the Secretary of Education at the Department of Education (ED), and where applicable, with the Secretaries of Health and Human Service (HHS), Agriculture (USDA), and Housing and Urban Development (HUD). The Plans are submitted online via the WIOA State Plan Portal system (WIOA SPP) that is used by nine program offices in five federal agencies: ED, DOL, HHS, HUD, and USDA.

The portal’s structure follows the Required Elements for Submission of the Unified or Combined State Plan and Plan Modifications under the Workforce Innovation and Opportunity Act (OMB Control Number 1205-0522). The State Plans are initially created and submitted by state users. The plans are then reviewed by teams of federal reviewers and approved by the Secretaries of the relevant agencies, or their designee(s). Once approved, the state plans are published on the WIOA State Plan Portal for public access.

This system is developed and maintained by the Office of Career, Technical, and Adult Education (OCTAE). The WIOA State Plan Portal will display the WIOA State Plans that describe how a State will address the statutory requirements of the Workforce Innovation and Opportunities Act and keep records of the plans available for public access.

Selected State users will be entering the state plans into the system; however, user account information is not be made available to the general public. Federal Reviewers will be reviewing State plans; based on their assigned workloads and will be able to see the status of each of the plans.

1.2. Describe the purpose for which the personally identifiable information (PII) is collected,

---

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
used, maintained or shared.

PII will be collected to enable account creation for Federal Users and a limited number of State Users that have been approved and authenticated by Federal staff. Accounts will be used to enter in narrative responses to questions regarding the States use of federal funding for WIOA programs.

State and Federal users will be required to log in, in order to enter in information for the State Plans. The accounts will enable users to enter in specific information into the system regarding their State’s response to the statutory requirements under WIOA.

The State users access the State Plan Portal to enter in their respective program information as part of the Workforce Innovation and Opportunity Act (WIOA), which is then sent for federal review and approval. Federal users review and approve each State’s program plan information, then may send it back to the State for more information/corrections or will send it to the next level of Federal approval and so on as described in question 1.1 above. The WIOA State Plan system will document the State’s plans as they relate to WIOA and any comments and edits based on the Federal Review of the State Plans.

1.3. Is this a new system, or one that is currently in operation?

New 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

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
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.

- Workforce Innovation and Opportunity Act (WIOA); July 22, 2014 (Pub. L. 113-128) 

**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

A system of record notice is not needed because the information collected is not retrieved by any personal identifiers. Records are retrieved by State or Federal agency.

**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 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](https://connected.ed.gov/om/Documents/SORN-Process.pdf)
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.

The Department shall submit a retention and disposition schedule that covers the records contained in this system to the National Archives and Records Administration (NARA) for review. 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.

Work email, first name, last name, office phone number, and State or Federal agency.

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

Yes

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

PII comes directly from the individual during account creation.

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

Federal and State users complete and submit the Request Access webform.
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?

PII is validated by checking with Federal Program Staff before approving access. State user accounts will be reviewed and re-validated at the beginning of every State Plan submission cycle. Users also can update their profile at any time. Federal User Approvers validate user requests according to lists of State grantees who receive WIOA funding. This list is provided by State Directors who administer the WIOA grants to Federal User Approvers.

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

The information is collected to create an account, assign roles and scope within the state plan workflows, and access the WIOA State Plan Portal website to enter or review the State Plans.

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.

---

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

The Privacy Notice is provided on the WIOA State Plan Portal account creation page prior to collection of the PII.

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

Privacy Notice:

Under the Workforce Innovation and Opportunity Act (WIOA) (Pub. L. 113-128), the Governor of each State must submit a Unified or Combined State Plan to the Secretary of the U.S. Department of Labor that outlines a four-year strategy for the State’s workforce development system. States must have approved Unified or Combined State Plans in place to receive funding for core programs (OMB Control Number 1205-0522).

Federal and State users who manage the WIOA programs are required to create an account to enter or review State Plans in the system. Users with WIOA State Plan Portal accounts can check on the status of a submitted material or upload new materials to the WIOA State Plan Portal.
For certain Federal and State users who need access to administrative privileges in order to carry out WIOA State Plan Portal functions in their roles as official representatives of federal, state, local or tribal governments or certain non-governmental organizations, the WIOA SPP website collects additional information such as work email, first name, last name, office phone number, and State or Federal agency. Submission of any information is voluntary and is being done purely for the purpose of authentication.

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?

Providing PII for account creation is voluntary but necessary to perform the duties or uploading State Plan information. State and Federal users who request access to the system to enter in State Plan information must agree to all terms of use before they provide the minimal PII.

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?

- [X] N/A

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

- [X] 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

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

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

\(^4\) 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.
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?

Users may view their information on their profile page on the WIOA State Plan System Website, once they are logged in. Users can contact their Federal liaison for more information.

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

Users may edit information on their profile page at any time after logging into the WIOA State Plan System website.

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

Users will be trained on the new State Plan Portal and provided instructions on how to correct their information. Users will also have a Resource page for additional instruction/training 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?
7.4. What administrative, technical, and physical safeguards are in place to protect the information?

Access to the system is controlled by a group of approved users who have received training unique to their responsibility of reviewing access requests and granting or denying access to the system. Accounts are blocked upon inactivity, upon request or if the system is accessed not in accordance to the Rules of Behavior. System owners review account management policy annually to ensure alignment with applicable policies, rules and regulations. Security awareness training for the federal user approvers is managed by the overseeing federal agency (Departments of Education, Labor, etc.). Contractor staff completes Security Awareness Training managed by the Department of Education quarterly.

All non-public facing information is protected by a role-based access control system which prevents unauthorized access. All logged in users are logged and tracked with unique ID’s. Passwords are hashed. All data is stored encrypted on disk, and in transit.

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.

All data and PII is encrypted in transit and at rest. Access to PII is only accessible to the owner (authorized logged in users), users with highly privileged application access, and developers who have server admin access. Content is monitored and logged for any changes along with the user who initiates the change. Physical access to devices is protected and monitored.
Additional monitoring includes monthly operating system vulnerability scans, database benchmark scans, web application vulnerability scans, and cloud and hosted application scans. The contractor can provide on-demand scans as needed within 14 days of request.

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 contractor to ensure the data is encrypted at rest and in motion using encrypted discs on the servers and through Secure Socket Layer/Transport Layer Security transport protocols.

The System Owner also ensures continuous implementation of the Risk Management Framework controls.

Training is provided to users for proper and secure use of the system. The System Owner audits Privileged Users annually and ensures they are properly trained and abide by the Rules of Behavior.

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?

We believe the most likely risks would present as fraud and identity theft. The application collects minimal information, but it does relate to the agency they work for, and that information could be used by various phishing and possibly gathering more information on that user. The application ensures authenticated and secure connections to mitigate a man in the middle attack. Passwords are hashed with salt, substantially lowering the success rate at discovering passwords. User accounts will be reviewed on an annual basis by Federal staff.