Privacy Impact Assessment (PIA)

for the

Workforce Innovation and Opportunity Act State Plan Portal

May 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: Mary Jo Maralit/System Owner
Contact Email: maryjo.maralit@ed.gov

System Owner

Name/Title: Mary Jo Maralit/System Owner
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 Workforce Innovation and Opportunity Act (WIOA) State Plan Portal (SPP) is developed and maintained by the U.S. Department of Education's (Department) Office of Career, Technical, and Adult Education (OCTAE) with an Interagency Agreement with the U.S. Department of Labor (DOL) to support requirements for the Workforce Innovation and Opportunity Act (WIOA), signed into law on July 22, 2014. WIOA is designed to help job seekers access employment, education, training, and support services to succeed in the labor market and to match employers with the skilled workers they need to compete in the global economy.

Under WIOA Public Law 113-128, States are required to submit State Plans to DOL. The State Plans are shared with the Department, and, where applicable, with the U.S. Department of Health and Human Services (HHS), the U.S. Department of Agriculture (USDA), and the U.S. Department of Housing and Urban Development (HUD). Plans are shared with the three partner agencies when States choose to include any of the combined partner programs listed in the WIOA statute.

States must have federally approved State Plans[1] to receive funding under six core programs (Adult, Dislocated Worker, Youth, Adult Education and Family Literacy Act (AEFLA), Wagner-Peyser, and the Vocational Rehabilitation (VR) programs). WIOA requires that States review their plan every two years and update State Plans based on changes in the labor market and economic conditions or other factors affecting the implementation of the State Plan. The plan requirements improve service integration and ensure that the workforce system is industry-relevant by responding to the economic needs of the state and matching employers with skilled workers. The State Plans describe how the state will develop and implement a unified, integrated service delivery system.

The State Plans are submitted via the WIOA SPP web application that is used by nine program offices in five Federal agencies (the Department, DOL, HHS, HUD, and USDA). The portal's structure follows the DOL information collection titled, Required

[1] Examples of guidance to grantees regarding State Plans:
• U.S. Department of Education, Office of Career, Technical, and Adult Education: https://www2.ed.gov/about/offices/list/ovae/pi/AdultEd/octae-program-memo-20-1.pdf
• U.S. Department of Education, Office of Special Education and Rehabilitative Services: https://rsa.ed.gov/sites/default/files/subregulatory/tac-20-01.pdf
• U.S. Department of Labor: https://wdr.doleta.gov/directives/attach/TEGL/TEGL_10-19.pdf

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). WIOA requires the governor of each state to submit a State Plan that includes a four-year strategy and operational plan for the continuing implementation of the state's workforce development system, with an update after two years.

The State Plans are initially created and submitted by state grantees and stored in the WIOA SPP. The plans are then reviewed in the WIOA SPP by teams of federal reviewers from the agencies listed above and approved by the Secretaries of the relevant agencies or their designee(s). The approved plans are published on the public facing WIOA SPP website.

The WIOA SPP has a password-protected area where state representatives can draft, review, and submit their plans and federal staff can review and provide comments by logging into the web portal with user accounts limited to their specific roles and duties. State Plans and user information are stored in the portal's secured database.

The WIOA SPP web portal is comprised of a webserver, application server, and database that comply with all security and privacy policies and regulations.

Users are identified by federal staff to create accounts in the WIOA SPP system. Once account creations are submitted, the system will validate the user's email address against the lists of acceptable Fully Qualified Domain Name (FQDNs). An email is sent to the users to verify the account creation request, once the account is verified, the user can update their password.

Once accounts are validated, federal staff review requests for additional roles prior to granting access. Roles for state users are state staff editor, state plan director, or big submitter for the state to which they are aligned. Roles for federal users include user approver, federal reviewer, federal program specialist, and federal panel lead.

1.2. Describe the purpose for which the personally identifiable information (PII)[2] is collected, used, maintained or shared.

PII (first name, last name, work email address, work phone number, and federal or state agency) is collected to enable account creation for designated federal users and a limited number of state users that have been approved and authenticated by federal staff.

[2] 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

State and federal users are required to authenticate into the WIOA SPP to complete their work on State Plans as described in question 1.1 above.

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

The PIA is being updated as part of the required biennial review.

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.

WIOA SPP is authorized by law to collect and use these data under the Workforce Innovation and Opportunity Act (WIOA) (29 U.S. Code Section 3101); 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)).[3] 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

State Plan information is retrieved by state. No information is 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.

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.

OCTAE is waiting on the 21st Century Information Retention Policy Framework to be approved and implemented. In that Framework, WIOA SPP would fall under DAA-0441-2022-0001-0002 II.A. Completed Research and Statistical Program Records.

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

[3] 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

2.4. 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.

The PII maintained within WIOA SPP includes name, work email address, office phone number, and state or federal agency as part of account creation for all authenticated state and federal users.

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 WIOA SPP for account creation and to allow for communication with authenticated state and federal users.

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

The sources of the information are the state and federal users who require access to the WIOA SPP.

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 for Account Access” form through the WIOA SPP in order to create an account for access.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[4] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

Federal user approvers validate user requests according to lists of state grantees who receive WIOA funding. 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.

Annual audits of user roles and permissions is conducted by the Information System Owner (ISO) as part of the ongoing security authorization process.

Use

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

In order for the states to submit their State Plans to DOL, the information is collected to enable account creation, assign roles, and scope within the State Plan workflows, and access the WIOA SPP website to submit 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.

[4] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

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.

Notice is provided on the WIOA SPP 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

Under the 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 SPP accounts can check on the status of a submitted material or upload new materials to the WIOA SPP.

For certain federal and state users who need access to administrative privileges in order to carry out WIOA SPP 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

Staff at the Office of Special Education and Rehabilitative Services have access to user information within the portal. Each office is responsible for reviewing and validating state and federal user accounts, based on the programs that they administer.

5.2. What PII will be shared and with whom?

☑ N/A

Department users will see the name, role, and email address of the members of their team.

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

☐ N/A

Federal teams need to coordinate and collaborate on the development and review of State Plans with each other and with the state teams.

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.

Yes

Staff at the DOL, HHS, HUD, and USDA have access to user information within the portal. Each office is responsible for reviewing and validating state and federal user accounts, based on the programs that they administer.

5.5. What PII will be shared and with whom? List programmatic disclosures only.[5]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

Federal users will see the name, role, and email address of the members of their team. State users will see the names and role of the people on their state team. Special state users, state program directors, and special federal users, user approvers, will see name, phone, and email for users requesting access to their programs.

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

☑ N/A

Federal teams need to coordinate and collaborate on the development and review of State Plans with each other and with the state teams.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

Sharing of information with the entities listed above is authorized by the Workforce Innovation and Opportunity Act.

[5] 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.

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

☐ N/A

Yes

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

☐ N/A

Users can only view PII by logging in to the WIOA SPP. Once they are authenticated, they can view their team members information. Information is not disseminated.

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

Yes

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 SPP 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 SPP website.

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

Webinars are provided for users of the WOIA SPP system. There are job aids on how to create and update account information on the WIOA SPP Resource page.

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?

WIOA SPP 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.

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 with the rules of behavior. System owner reviews 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. Contractor staff completes security awareness training managed by the Department 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 IDs. 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 system admin access to the portal. 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.

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 WIOA SPP 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 WIOA SPP 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 WIOA SPP 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.

WIOA SPP 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.