Employment and Training Administration

Office of Unemployment Insurance

Unemployment Insurance Reporting System (UIRS)

PRIVACY IMPACT ASSESSMENT

October 2024

☑ Concurrence of Senior Agency Official for Privacy
☐ Non-concurrence of Senior Agency Official for Privacy

Carolyn Angus-Hornbuckle

Digitally signed by Carolyn Angus-Hornbuckle
Date: 2024.11.22 15:37:57 -05'00'

Carolyn Angus-Hornbuckle, Senior Agency Official for Privacy
Assistance Secretary for Administration and Management

Table of Contents

PRIVACY IMPACT ASSESSMENT

1. OVERVIEW

Currently, the U.S. Department of Labor (DOL) Employment and Training Administration (ETA) provides states individual servers, that are physically located on state premises. States utilize the servers to upload and communicate Unemployment Insurance (UI) program related performance and evaluation data to ETA's reporting mainframe database. The state data is uploaded and stored in ETA's Unemployment Insurance Database Management System (UIDBMS). As described in this PIA, the UIDBMS is being overhauled and replaced with a new system called the Unemployment Insurance Reporting System (UIRS). Historically under UIDBMS, there has been a separation of the state servers and any database managed by DOL. Under the UIRS, the data provided by states will be uploaded directly to a cloud-based database managed by the DOL's Office of the Chief Information Officer (OCIO) and hosted by a third-party vendor contracted by OCIO.

The major objectives of the UIRS modernization initiative are to eliminate physical servers, migrate reporting data to the cloud, and enhance data validation at the point of input to avoid errors, thereby improving state data collection, access management for better data security, and data design. With this modernization, both the state and DOL regional and national applications will be on the same infrastructure within the new modernized UIRS.

The state data that contains personally identifiable information (PII) will be uploaded to and hosted on a DOL managed secure cloud server.

This PIA describes the users that will have access to the data in the UIRS and the limitations of that access. Generally, users will be limited to only the level of access that their role requires and only access the type of information in the UIRS that is necessary for the user to conduct their business. For example, a State Business User, a Regional/National DOL Business User, and a DOL or Vendor Technical Team User would only have the following access:

> ***State Business Users***: these users only have access to their state's data in the UIRS as is currently the practice. The states will determine and submit authorized users to the DOL. DOL program staff authorized to approve state business users will instruct OCIO to grant access to authorized users on the application level.
>
> ***Regional/National DOL Business Users***: these users will only see aggregate-level data, not any state-specific PII data. Access will be controlled via user roles and access control as determined by authorized DOL staff (OUI) and shared with OCIO security team.
>
> ***DOL or Vendor Technical Team Users***: The tables/files that hold PII data are only accessible to these users that have access to the cloud components on an as needed basis. The access is restricted using authorization, monitoring, and encryption as determined by the OCIO security team.

The UIRS is part of a wider effort to modernize UI systems and processes. The UIRS is owned by the Office of Unemployment Insurance (OUI) within DOL's ETA and furthers the ETA's mission of providing leadership, oversight, direction, and assistance to state UI agencies in the implementation and administration of state UI programs.

The UIRS will be used by DOL to collect aggregate data from states. It will not collect data or PII directly from UI claimants. However, states will have the ability to upload to the UIRS certain individual level data that could include PII as well as individual level demographic, employment, and wage data regarding UI claimants when such data falls within the scope of required reports to the Department. As mentioned above, the Department will have limited ability to access the PII uploaded by states.[1] Generally DOL's access to data will be through a separate interface that only deals with anonymized, aggregated data.

The UIRS has the following components:

- User Interface (UI): Developed on the Salesforce platform, provides a customizable environment that supports state and national systems administrators in managing reports and operations efficiently.

- Database Management System (DBMS): Utilizes Salesforce for transactional data handling and AWS for scalable data storage solutions, ensuring robust data management capabilities.

- Application Server: Hosted on Salesforce, this component processes all business logic, facilitating data communication between the user interface and the databases.

- Web Server: Also integrated within Salesforce, this server manages web sessions, security checks, and the delivery of web content to users.

- Identity and Access Management (IAM): Managed through Salesforce and supplemented by Azure Active Directory and Login.gov for state user account authentication (i.e., multi-factor authentication) to prevent unauthorized use of an authorized user credential to enhance security.

- Audit and Compliance Monitoring Tools: The Salesforce-maintained platform includes a set of federal and industry standard compliance certifications and attestations to validate and support IT auditing and reporting functions. The platform is used to generate and review monthly audit reports for the OCIO security team. These reports include all activities and user actions performed on the UIRS application(s) during the month.

[1] As noted throughout this PIA, DOL or Vendor Technical Team Users will have access to the PII in the system as a necessary part of system administration and maintenance, but individuals granted this type of access will be strictly and tightly controlled by DOL's OCIO security team.

- Security Infrastructure: Includes Salesforce Government Cloud and Salesforce Shield for comprehensive security measures such as firewalls, intrusion detection systems, and advanced data encryption to protect data in transit and at rest.

The states are responsible for complying with all program performance and evaluation reporting requirements and the use and operation of the UIRS does not change any such existing or future obligations under the law, regulation, grant agreements, or pursuant to other agreements between states and DOL.

This PIA is being conducted for the UIRS because states will upload PII to a DOL-controlled system.

2. CHARACTERIZATION OF THE INFORMATION

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, or technology being developed.

- **From whom is information to be collected?**

  Information is being collected from states as part of each state's reporting obligations under 20 CFR Part 602.

- **Why is the Information being collected?**

  Under the statutes and regulations that implement and direct the state UI system, states are required to report data to ensure timely and accurate payment of benefits and to provide internal quality assurance information to help ensure the proper and quality administration of UI programs. The data transmitted to DOL will be used to identify errors in claims processes and revenue collections, analyze causes, and support the initiation of corrective action. The data will also be combined with other information for statistical and other analysis such as assessing the impact of economic cycles, funding levels, and workload levels on program accuracy and timeliness.

- **What is the PII being collected, used, disseminated, or maintained?**

  States are responsible for collecting data, including PII, that relate to an individual's eligibility for UI benefits, data that is necessary for the operation of the UI program, and data needed to conduct proportions tests to validate the selection of representative samples (the demographic data elements necessary to conduct proportions tests are claimants' date of birth, sex, and ethnic classification). Thereafter, states are required to furnish information and reports to DOL, including weekly transmissions of case data entered into the UIDBMS/UIRS, without, in any manner, identifying individuals to whom such data pertain. Although DOL plans to collect expanded demographic data to comply with OMB's Statistical Policy Directive No. 15[2] in the future, it will still receive only the aggregated information from states, not PII. This list may be updated, where needed, as future modules or program applications of the UIRS system are deployed to production. Any data that is constituted as confidential UC information and will be handled and stored in compliance with 20 CFR Part 603.

☒ Name
☐ Middle Initial
☐ Date of birth

☐ Place of birth
☐ Mother's maiden name
Maiden name
☒ SSN (full)

[2] Federal Register: Revisions to OMB's Statistical Policy Directive No. 15: Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity

☐ SSN (truncated)
☐ Race
☐ Ethnicity
☐ Gender
☐ Sex
☐ Disability status
☐ Religion
☐ Language spoken
☐ Military, immigration, or other government-issued identifier
☐ Photographic identifiers (e.g., photograph image, x-rays, video)
☐ Biometric identifier (e.g., fingerprint, voiceprint, iris)
☐ Other physical identifying information (e.g., tattoo, birthmark)
☐ Vehicle identifier (e.g., license place, VIN)
☐ Driver's license number
☐ Residential address
☐ Personal phone numbers (e.g., phone, fax, cell)
☐ Mailing address or P.O. Box
☐ Personal email address
☐ Business address
☐ Business phone number (e.g., phone, fax, cell)
☒ Business email address
☐ Medical information
☐ Medical record number
☒ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
☐ Financial account information and/or number
☐ Birth, Death, or Marriage Certificates
☐ Legal documents or notes (e.g., divorce decree, criminal records)
☐ Educational records
☐ Network logon credentials (e.g., username and password, public key certificate)
☐ Digital signing or encryption certificate
☒ Other: Some types of individualized demographic data may be uploaded by states for their own use.

- **How is the PII collected?**

  States are responsible for collecting data as necessary, including PII, for the operation of the UI program, and for DOL mandated reporting and quality control activities. States establish and maintain their own secure system of records and provide DOL aggregate information for reporting purposes only. DOL's access to PII is authorized on an as needed basis only and is restricted using authorization, monitoring, and encryption. The UIRS functions as the central location for states to upload certain data needed to prepare required reports. DOL is able to access the reports that contain aggregate information, but DOL is unable to query the UIRS for individual wage records and data containing PII. UIRS functions as the central location for states to upload certain data that they will need to work on.

  States interact with the UIRS using role-based access controls within a unified system hosted on the DOL AWS Cloud platform. Previously, states operated separate systems with data transferred via physical servers and batch processing. Now, the UIRS integrates both federal and state systems into a single cloud-based environment. This setup allows states to manage their data directly within the UIRS through distinct permissions and roles, ensuring that they function within the same ecosystem while maintaining separate controls over their specific data. This architecture eliminates the need for separate systems and streamlines the data management process across different governmental levels.

- **How will the information collected from individuals or derived from the system be checked for accuracy?**

  States are responsible for determining the accuracy of the information for reporting and evaluation purposes.

- **What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?**

  Title III of the Social Security Act (SSA), 42 U.S.C. 501-503; the Federal Unemployment Tax Act (FUTA), 26 U.S.C. 3304; Section 2118 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act (Pub. L. 116-136), as amended; Section 410(a) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Stafford Act) (42 U.S.C. 5177(a)); The Unemployment Compensation for Ex-Service Members (UCX) law and The Unemployment Compensation for Federal Employees (UCFE) law (5 U.S.C. Chapter 85); Chapter 2 of Title II of the Trade Act of 1974 (19 U.S.C. 2271 et seq.), as amended; and 20 CFR parts 602, 603, and 604.

- **Privacy Impact Analysis**

  The UIRS addresses the risks of storing and transmitting data that may contain claimant PII by employing robust safety controls to protect against unauthorized access to data at rest and interception of data in transit. To mitigate unauthorized access to data at rest, the system utilizes Salesforce Shield to encrypt all PII in a separate data store from transactional, non-PII data, ensuring that data remains secure when it's not actively being used. For data in transit, PII submitted by states is secured using Transport Layer Security (TLS) protocols for HTTPS communications, supplemented by mutual TLS (mTLS) to authenticate both ends of data transfers. Additionally, the UIRS leverages the DOL AWS Cloud platform, which supports these encryption efforts with its own comprehensive security measures including role-based access control (RBAC) to regulate who can access the system based on their roles, and detailed audit logs that monitor and record all system interactions to detect and respond to potential security threats effectively. These strategies collectively ensure that the UIRS maintains high levels of data integrity and confidentiality.

3. DESCRIBE THE USES OF THE PII

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

- **Describe all the uses of the PII.**

  States are responsible for collecting data, including PII, that relate to an individual's eligibility for UI benefits, data that is necessary for the operation of the UI program, and data needed to conduct proportions tests to validate the selection of representative samples. DOL or Vendor Technical Team Users will have access to state PII data on an as needed basis only and is for system administration and maintenance, and this access is tightly controlled and restricted using authorization, monitoring, and encryption. DOL relies on aggregated data to conduct its state performance and quality evaluations. States will be able to access only the data points that they upload into UIRS and will use that data to prepare the reports for DOL. No state will be able to access the individual data uploaded to the UIRS from another state.

- **What types of tools are used to analyze data and what type of data may be produced?**

  Salesforce primarily handles the front-end interaction and database management, leveraging its Customer Relationship Management (CRM) system for data tracking, user engagement, and reporting. This includes using Salesforce Lightning for creating engaging user interfaces and Salesforce Shield for ensuring data security through encryption and detailed event monitoring. On the backend, AWS offers comprehensive support with services like AWS Lambda for efficient serverless computing, Amazon S3 for scalable storage solutions, Amazon RDS for reliable relational databases, and AWS Batch for managing large-scale processing jobs. This integrated approach ensures a seamless flow of data between user interaction points managed by Salesforce and the heavy lifting of data processing and storage handled by AWS, allowing for a sophisticated and comprehensive data analysis and management system.

- **Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?**

  Data is aggregated by states before DOL business users access it. Data will not be derived for individuals, but rather will be aggregated at population levels.

- **If the system uses commercial or publicly available data, please explain why and how it is used.**

  The system does not use commercial or publicly available data.

- **Will the use of PII create or modify a "system of records notification" under the Privacy Act?**

  No. There will be no built-in capability to retrieve data from the UIRS using personal identifiers.

- **Privacy Impact Analysis**

  The operational storage and use of PII can create the risk of unauthorized access and disclosure. The PII stored in the UIRS cloud environment is subject to a moderate security risk and is hosted in a cloud environment with implementation of the NIST Moderate baseline security controls for a Moderate system as recommended by National Institute of Standards and Technology (NIST) SP 800-53, Recommended Security Controls for Federal Systems. NIST controls are specifically designed for cloud environment projects and are more stringent than controls for non-cloud projects. Additionally, all PII that constitutes confidential UC information will be handled and stored in compliance with 20 CFR Part 603.

4. RETENTION

The following questions are intended to outline how long information will be retained after the initial collection.

- **What is the retention period for the data in the system?**

  DOL will prepare a record retention policy for approval through the National Archives and Records Administration (NARA). Until such policy is approved, the records will be maintained indefinitely.

- **Is a retention period established to minimize privacy risk?**

  The NARA retention period to be selected for these records will help minimize privacy risks, and ensure records are not held longer than necessary, as well as to ensure compliance with federal confidentiality regulations regarding UI-related data (see 20 CFR Part 603).

- **Has the retention schedule been approved by the National Archives and Records Administration (NARA)?**

  No.

- **Per OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, what efforts are being made to eliminate or reduce PII that is collected, stored, or maintained by the system if it is no longer required?**

  States will upload individual level demographic, employment, and wage data containing PII to the state-side portion of UIRS that will be necessary for the state to complete its aggregate reporting for DOL. States will be able to remove/replace the data they provided to the UIRS, including data containing PII, at any time and when the purpose for which it was uploaded (e.g., performance reporting, quality assurance review) has been satisfied.

- **How is it determined that PII is no longer required?**

  PII is no longer required to be stored in the UIRS when the purpose for which the data was uploaded has been satisfied (e.g., at the conclusion of the quality assurance review, etc.), and in compliance with the NARA retention schedule, as appropriate.

- **If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.**

  DOL or Vendor Technical Team Users will have access to state data containing PII on an as needed basis only (for system administration and maintenance) and is restricted to using authorization, monitoring and encryption. DOL relies on aggregated data to conduct its state performance evaluations.

In situations where it is not possible to completely remove PII from the system, OwnBackup plays a key role by ensuring that users do not see real PII data in testing and development environments, like sandboxes. OwnBackup does this by either removing PII or replacing it with dummy values. This means when developers or testers are working, they are using data that looks real but does not expose any private information. This approach helps protect people’s privacy by making sure their data is not accidentally seen or misused during system updates or when new features are being developed.

- **Privacy Impact Analysis**

  Longer data retention increases the likelihood that larger amounts of PII are exposed. To mitigate the risk of exposure, the UIRS team will adhere to the pending NARA data retention requirements for data collected under UIRS.

5. INTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the scope of sharing within the Department of Labor.

- **With which internal organization(s) is the PII shared, what information is shared, and for what purpose?**

  The PII data is not shared with other internal DOL organizations, except to the extent required by law.

- **How is the PII transmitted or disclosed?**

  PII is not transmitted, disclosed, or available for viewing to any party other than the state that uploaded the data into the UIRS, unless required by law, and in limited circumstances, to DOL or Vendor Technical Team Users on an as needed basis. DOL access to PII (for system administration and maintenance) and is restricted using authorization, monitoring, and encryption. Only aggregate data is transmitted to DOL thereafter.

- **Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?**

  Not applicable.

6. EXTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the content, scope, and authority for information sharing external to DOL which includes federal, state, and local government, and the private sector.

- **With which external organization(s) is the PII shared, what information is shared, and for what purpose?**

  No data with PII is shared with external organizations. Reports generated from DOL analyses based on state aggregate data are publicly available on DOL's UI Data Page website https://oui.doleta.gov/unemploy/DataDashboard.asp. The reports contain aggregated data in an anonymized format; no PII is present.

- **Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.**

  No data with PII is shared with any external organizations.

- **How is the information shared outside the Department and what security measures safeguard its transmission?**

  Although there will be some sharing of information in reports by Regional/National DOL Business Users, it will be aggregated and not include the state-specific PII. The DOL or Vendor Technical Team Users that have access to the system for system administration and maintenance purposes will not share PII outside DOL.

- **How is the information transmitted or disclosed?**

  No data with PII is transmitted or disclosed outside DOL. As noted above, DOL access to PII in the system is either restricted or limited to system administration and maintenance which will not involve transmission or disclosure of PII.

- **What type of training is required for users from agencies outside DOL prior to receiving access to the information?**

  DOL will be providing State UI Agencies with training on how to upload their data to UIRS. State users must establish an account, agree to the Rules of Behavior, and review the program user guides for each application on the UIRS before receiving access. DOL will host a series of webinars, upload program specific user guides/demonstration videos/transcripts and provide other resource material as it becomes available online to the UI Community of Practice for the UIRS on ETA's Workforce GPS. Information on these training resources will be disseminated to states through ETA's Regional offices and on its public website. However, only state workforce agency staff, with the approval of their state administrator, will be able to access the training information on Workforce GPS or establish a UIRS account.

- **Privacy Impact Analysis**

  A state has access to the PII that it uploads into the UIRS, but no other state or DOL will have access to that data. Once a state has completed its required reporting using its data, the data that is shared with DOL is only aggregate level data. As described throughout this PIA, DOL uses a combination of software and access controls to add additional protection and to avoid any accidental viewing or sharing of PII from the UIRS.

7. NOTICE

The following questions are directed at notice to the individual of the scope of PII collected, the right to consent to uses of said information, and the right to decline to provide information.

- **Was notice provided to the individual prior to collection of PII?**

  Section 303(a)(1) of the Social Security Act (SSA), 42 U.S.C. 503(a)(1), requires that a State law include provision for: "Such methods of administration . . . as are found by the Secretary of Labor to be reasonably calculated to insure full payment of unemployment compensation when due." This includes states furnishing individuals who may be entitled to unemployment compensation such information as will reasonably afford them an opportunity to establish claims and protect their rights under the unemployment compensation law of such State. Such information may include disclosure of PII to file a claim, manner and places of filing claims, the reasons for determinations, their rights of appeal, etc. Every state provides claimants its own Privacy and Security Notices.
  This Privacy Impact Assessment also represents a form of notice provided prior to the collection of PII.

- **Do individuals have the opportunity and/or right to decline to provide information?**

  The act of filing a claim is contingent upon the individual claimant providing necessary information, including PII per the state's Privacy and Security Notice.

- **Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?**

  No. There is no selective usage of claimant information. Filing for UI benefits will result in claimant information being collected by and disseminated to the state system where the claim was filed for the purpose of administering the UI program and DOL quality control. Only information necessary for the administration of the UI program is collected. Some of this information collected by states will be uploaded to the state-only access location in the UIRS. DOL will not have access to this individual-level data.

- **Privacy Impact Analysis**

  Individuals receive notice that their claim information may be used for other purposes in several ways, including the federally required notices that all claimants receive from a state when filing their UI claims in accordance with 20 CFR section 603.11 and the publication of this PIA which describes the state use of claimant information for reporting purposes. Employers also receive notices from states regarding this use of wage information. For reporting and quality control purposes, states submit PII and aggregate information to DOL for oversight and analysis. DOL or Vendor Technical Team Users will have access to state PII data on an as needed basis only (for system administration and maintenance) and is restricted using authorization, monitoring, and encryption.

8. INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about them.

- **What are the procedures that allow individuals to gain access to their own information?**

  Not applicable. Individuals will not have access to the UIDBMS/UIRS. For any claim/individual level inquiries, individuals must contact their state workforce agency.

- **What are the procedures for correcting inaccurate or erroneous information?**

  Not applicable. Individuals will not have access to the UIDBMS/UIRS. For any claim/individual level inquiries, individuals must contact their state workforce agency.

- **How are individuals notified of the procedures for correcting their own information?**

  Not applicable. Individuals will not have access to the UIDBMS/UIRS. For any claim/individual level inquiries, individuals must contact their state workforce agency.

- **If no formal redress is provided, what alternatives are available to the individual?**

  For any claim/individual level inquiries, individuals must contact the state workforce agency where their claim is filed.

- **Privacy Impact Analysis**

  Individuals will have the right to access, modify, and amend their information at the state level. The states have existing processes for access and modification requests by individuals. Therefore, redress-related risks are mitigated by existing procedures at the state level to ensure accurate and complete claims information.

9. TECHNICAL ACCESS AND SECURITY

The following questions are intended to describe technical safeguards and security measures.

- **Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)**

  At the time of the initial release in June 2024, there will be select State Business Users and Regional/National DOL Business Users that will be provided access to the Data Validation (DV)/Tax Performance System (TPS) application. The authentication is going to be enforced via Login.gov or via Azure Active Directory. The authorization will be configured for those users based on their roles. State Business Users are vetted by the respective state. Authorized DOL Regional/National Business Users also must have a Personal Identity Verification (PIV) card to log in to DOL-issued computers before being able to access the DV and TPS modules of the application.

  The State Business users will perform functions related to the DV and TPS modules of the application. The DV functions include uploading population (audit data) files, conducting validation activities, and submitting results to the DOL National Office. For TPS, the actions include sampling, computed measure verification and program performance reviews. Regional/National DOL Business Users then access the system to verify the aggregate results for both DV and TPS, which does not contain any PII, and identify areas for oversight/monitoring, technical assistance, or training for State UI programs.

- **Will contractors to DOL have access to the system?**

  Yes, there are a limited number of system administration professionals that may encounter protected data as necessary to execute required system maintenance functions as contracted support services.

  During the onboarding process for all contract employees that will be interacting with UIRS, individuals undergo background checks and training on data security and confidentiality. In addition, all contractors sign a non-disclosure agreement that outlines contractor responsibilities, including compliance with DOL policies and regulations governing the handling, protection, and destruction of sensitive information and 20 C.F.R. Part 603; protection of authentication devices and access credentials; reporting security incidents; prohibiting the unauthorized use and release of information; and protecting the integrity of DOL systems and equipment.

- **Does the system use “roles” to assign privileges to users of the system? If yes, describe the roles.**

  Yes, the system uses roles to assign privileges to users of the system. Access to functions and data within the system are restricted by roles granted to them within the DV/TPS application.

- **What procedures are in place to determine which users may access the system and are they documented?**

  User access rights will follow the access control standard operating procedures which are documented in DOL procedures. Additionally, access will be further controlled by requiring users to go through Single Sign-On (SSO) using either Login.gov or Azure Active Directory. This means a user must first be set up with SSO through one of these platforms to gain access, ensuring another layer of security and verification for user identity.

  Standard operating procedures guide the methods and procedures used by DOL or Vendor Technical Team Users when accessing the system for maintenance purposes.

- **How are the actual assignments of roles and Rules of Behavior verified according to established security and auditing procedures? How often is training provided?**

  A standard operating procedure will be developed where the list of users and their roles will be provided to the state, regional, and national administrators to verify. The frequency of that exercise will be defined working with the Business Users.

  OCIO personnel and state IT personnel work together on an ongoing basis to maintain awareness of roles and Rules of Behavior.

  DOL will host a series of webinars, upload program specific user guides/demonstration videos/transcripts and provide other resource material as it becomes available for the UIRS online through the UI Community of Practice on ETA's Workforce GPS. The training will continually be available, and any new resources identified will be developed by OCIO and program office staff, as needed.

- **Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?**

  DOL UIRS users will be required to take the annual Cybersecurity and Privacy Awareness Training. Additionally, any DOL employees and contractors with access to the UIRS system will also receive training on handling UI information consistent with DOL's non-disclosure agreements with staff or contractor(s) using the system. Prior to deployment to production of future modules or program applications of the UIRS system that include "confidential UC information" as defined in 20 CFR Part 603): (1) the privacy training for all DOL users of this system will be expanded to include information on protections of and safeguards for any data that constitutes confidential UC information and such information will be handled and stored in compliance with 20 CFR Part 603; and (2) all non-disclosure agreements with staff or contractors (of the UIRS system) who may have access to such information will reference and describe such confidential UC information and the safeguards required by 20 CFR Part 603.

- **What auditing measures and technical safeguards are in place to prevent misuse of data?**

  All sensitive user data is encrypted at rest and in transit. The UIRS system employs multi-factor authentication combined with role-based authorization to safeguard the application. Only approved and privileged accounts have system access. Any sensitive data (such as PII) is encrypted so any party that does not explicitly require access or have a token to decrypt the data cannot access the data. In addition, the system is monitored specifically for data exfiltration events.

  The system also incorporates comprehensive Salesforce audit logs. These audit logs meticulously track user actions within the application, such as login attempts, data access, and changes made to the data. This enables a detailed review of user activities, helping to ensure accountability and detect any unauthorized or suspicious behavior.

- **Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?**

  Data within the UIRS is secured in accordance with Federal Information Security Management Act (FISMA) requirements.

- **Privacy Impact Analysis**

  The risk associated with collecting sensitive PII is exposure of that information. This risk is mitigated by implementing the access controls (least privilege access and zero-trust), technical controls (encryption at rest and transit), and physical controls (security) described in this PIA and engaging in a continuous monitoring of the controls applied to this system.

10. TECHNOLOGY

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, biometrics, and other technology.

- **Was the system built from the ground up or purchased and installed?**

  The system is built from the ground up on the DOL AWS cloud platform and Salesforce instance procured by DOL. DOL's AWS cloud has received an ATO. The third-party federal partner is a purchased platform-as-a-service. The web interface and web server are custom-built utilizing the PaaS solution.

- **Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.**

  Privacy and security considerations were utilized to make architectural and other technical decisions for the application. The application uses systems that have gone through the ATO process to ensure vetted controls could be inherited to its fullest extent. The application also used a Salesforce FedRAMP instance that inherits a lot of control due to this categorization. The PII and non-PII data are encrypted in transit and at rest with the minimum number of users or systems possible having the ability to decrypt the data. Data integrity is considered through the implementation of rigorous data checks using data objects.

- **What design choices were made to enhance privacy?**

  The UIRS system is being hosted on a FedRAMP platform utilizing Salesforce Shield for data encryption at rest. The solution is also using DOL's AWS cloud and is leveraging controls from it. The system is designed to encrypt information at every step of the process and minimizes the number of people and systems able to decrypt the information.

- **For systems in development, what stage of development is the system in, and what project development life cycle was used?**

  The system uses an agile software development process and is currently in the development phase in accordance with the DOL System Development Life Cycle Management Manual.

- **For systems in development, does the project employ technology which may raise privacy concerns? If so, please discuss their implementation?**

  The UIRS does not incorporate technology that might raise privacy concerns, as it avoids the use of open-source products. In its current iteration, the UIRS relies upon states to select authorized users for UIRS. UIRS uses Azure Active Directory and Login.gov for login authentication (i.e., multifactor authentication) to prevent unauthorized use of an authorized state user credential. DOL users have their identity verified through the onboarding process and issuance of a PIV card used to access DOL computers and systems. User credentials are then established for relevant DOL personnel who are given access to UIRS.

11. PIA SIGNATURE PAGE

Reviewed by: Jim Garner, Administrator, Office of Unemployment Insurance, ETA Representative

Digitally signed by JIMMIE GARNER
Date: 2024.11.11 09:58:26 -05'00'

Signature

Reviewed by: Mara Blumenthal, DOL Privacy Office

MARA BLUMENTHAL Digitally signed by MARA BLUMENTHAL
Date: 2024.11.19 14:08:15 -05'00'

Signature