Employment and Training Administration

Office of Unemployment Insurance

Unemployment Insurance Reporting System (UIRS)

PRIVACY IMPACT ASSESSMENT

November 2025

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

BRAYE CLOUD Digitally signed by BRAYE CLOUD

Braye Cloud, Senior Agency Official for Privacy
Deputy Assistance Secretary for Operations

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 owned, maintained, and managed by DOL's Office of the Chief Information Officer (OCIO), but 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 central reporting 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). Under the UIRS, the data provided by states will be uploaded directly to a cloud-based database administered by the DOL's OCIO and securely hosted by a third-party vendor contracted by OCIO.

The major objectives of the UIRS modernization initiative are to eliminate the cost and complexity of maintaining physical servers, mitigate technology risks inherent in the UIDBMS, migrate state 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, however, each state and DOL Business Users will only have compartmentalized access to data secured in the cloud infrastructure. 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 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 is used by DOL to collect program reporting data, including aggregate and de-identified, individual level data from state UI agencies. DOL will not collect personally identifiable information (PII) or other data directly from UI claimants. Upon implementation of UIRS Phase II, each state will upload data (specifically for the Benefits Accuracy Measurement or BAM program), that includes personally identifiable information (PII), to the new system. The individual level data could include UI claimants' demographic, employment, and wage information that is required to assess and determine the improper payment rate by the Department. However, as mentioned above, DOL's access to state-restricted data with PII will be limited to circumstances when it is required in order for DOL or Vendor Technical Team users to provide technical assistance/troubleshooting to state users (system administration and maintenance).[1] For programmatic purposes, the data containing PII will be accessible only to the State Business Users for the individual state that owns and uploads such data. DOL's access to data for program purposes will be through an interface that only includes deidentified or aggregated data.

[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.

The UIRS has the following components:

- User Interface (UI): Developed on the Customer Relationship Management (CRM) Tool platform, provides a customizable and compartmentalized environment that supports state and national systems administrators in managing reports and operations efficiently.
- Database Management System (DBMS): Utilizes CRM Tool for transactional data handling and DOL Cloud Platform for scalable data storage solutions, ensuring robust data management capabilities.
- Application Server: Hosted on CRM Tool, this component processes all business logic, facilitating data communication between the user interface and the databases.
- Web Server: Also integrated within CRM Tool, this server manages web sessions, security checks, and the delivery of web content to users.
- Identity and Access Management (IAM): Managed through a CRM Tool and supplemented by Active Directory and login authentication 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 CRM Tool-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.
- Security Infrastructure: Includes a CRM Tool Government Cloud and a CRM Tool 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 existing or future obligations under the law, regulation, grant agreements, or other agreements between states and DOL.

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. State Business Users, Regional/National DOL Business Users, and DOL or Vendor Technical Team Users will have the access needed for and appropriate to their respective roles.

This PIA is being conducted and updated prior to the Fall 2025 implementation of Phase II for the UIRS. At the time of Phase II implementation, states will begin uploading PII to this DOL system when two additional applications (BAM and UI Required Reports (UIR)) are added to the production version of the system. The BAM and UIR applications in the system are currently in development and anticipate the production version added to current UIRS architecture no later than the first calendar quarter of 2026.

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?**

  State UI agencies upload information, which includes data with PII that the state collects from individual UC claimants, to the UIRS. Following deidentification or aggregation, as appropriate, the state information becomes accessible to DOL Business Users as part of each state's reporting obligations, including BAM Reporting as required 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?**

  Under BAM, 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. DOL plans to continue to collect BAM data as approved under OMB Control No. 1205-0245.

  DOL Business Users will continue to receive only aggregate-level data, without PII, for the DV, TPS, and UIR applications. UIR Reports data is totaled and does not contain individual claimant or employer information. The BAM application will include only de-identified, individual level data (i.e., batch number indicating key week and sampled case sequence number for DOL Business Users). DOL Business Users will not be able to search by name, SSN, date of birth, or any other form of 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 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)
☒ SSN (truncated)
☒ Race
☒ Ethnicity
☒ 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 from UC claimants, including PII, as necessary for the operation of the UI program. Based on the individual level data that is selected by the state for uploading to the UIRS, each state submits aggregated and deidentified data via the UIRS as required for DOL mandated and quality control activities. States establish and maintain their own secure system of records and provide DOL with these records via the UIRS for reporting purposes only. DOL's access to PII is authorized on an as needed basis only and is restricted based on user role using authorization, monitoring, and encryption. The UIRS functions as the central location for states to upload certain data needed to prepare required reports and comply with the requirements of other UI programs.

States interact with the UIRS using role-based access controls within a central location hosted on a CRM Tool. Previously, under the legacy system, states operated separate systems with data transferred via physical servers and batch processing. Now, the UIRS hosts both federal and state systems in a single cloud-based environment. This setup allows states to independently 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 CRM Tool 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 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 relates 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 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 while fulfilling its oversight functions of state UI programs. However, the BAM program uses de-identified data to measure the integrity of state UI programs and determine improper payment rates as part of DOL's oversight, evaluation, and monitoring responsibilities. 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 in the UIRS from another state.

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

  A CRM Tool primarily handles the front-end interaction and database management, leveraging its system for data tracking, user engagement, and reporting. This includes creating engaging user interfaces and ensuring data security through encryption and detailed event monitoring. On the backend, the DOL Cloud Platform offers comprehensive support with services for efficient serverless computing, scalable storage solutions, reliable relational databases, and managing large-scale processing jobs. This integrated approach ensures a seamless flow of data between user interaction points managed by the CRM Tool and the heavy lifting of data processing and storage handled by the DOL Cloud Platform, 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?**

  No. Data is aggregated by states before DOL business users access it. Data will not be derived from 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" (SORN) under**

the Privacy Act?

No. There will be no built-in capability to retrieve data from the UIRS using personal identifiers and information is NOT retrieved by the name of the individual or by other personally identifiable information (i.e., SSN or date of birth), therefore no SORN is necessary.

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). State data in the UIRS should also be retained according to state specific statute of limitations or other data retention requirements (beyond those stipulated by DOL for a particular UI application or program). For instance, DV records should be maintained by states for at least three years while TPS records should be maintained by states for at least four years.

- **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 reporting for DOL. States will be able to remove and replace the data they provided to the UIRS (e.g., modify a report), 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?**

  Each state owns, maintains access, and manages the data lifecycle of the PII data that it uploads in the UIRS. PII will be subject to the applicable data retention requirements of the state that owns such data.

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.). Federal data retention for aggregate and deidentified data accessed by DOL Business Users for program reporting purposes will follow and comply 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.**

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. 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.

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. PII data will not be shared by or within DOL. The PII data in the UIRS belongs to and will only be accessible to the State Business Users of the state that upload such data to the UIRS. DOL Business Users will not have access to the PII data and therefore cannot share such data with internal organizations.[2] An organization that requires access to state data will be directed to seek such data from the state(s) directly.

- **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 for technical assistance. DOL access to PII (for system administration and maintenance) is restricted using authorization, monitoring, and encryption.

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

  Not applicable.

[2] As noted elsewhere in this PIA, DOL or Vendor Technical Team Users may have incidental access to the state-owned PII data as a necessary part of system administration and maintenance, but such technical access and the individuals granted this type of access will be strictly controlled by DOL's OCIO Security team.

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 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. Individual-level BAM program data is not publicly available.

- **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 not include 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 application, 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 in Workforce GPS or establish a UIRS account.

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, manners and places of filing claims, the reasons for determinations, their rights of appeal, etc. Each state provides claimants with 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?**

  In order to file an unemployment compensation claim, an individual must provide necessary information, including PII. Each state's Privacy and Security Notice advises claimants that the specified PII must be provided in order to proceed with a UC claim.

- **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 individual-level data that contains PII.

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?**

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

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

  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?**

  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 agency level. The states have existing processes for access and modification requests by individuals. Therefore, redress-related risks are mitigated by existing state agency procedures that 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, there will be select State Business Users and Regional/National DOL Business Users that will be provided access to the BAM and UIR applications, in addition to the DV/TPS application, in accordance with the roles described under Section 1 of this document. 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 application.

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

  Yes, there are a limited number of system administration professionals (DOL or Vendor Technical Team Users) that may encounter protected data when necessary to execute required system maintenance functions as contracted support services.

  During the onboarding process, all DOL employees and contracted staff that will be interacting with UIRS undergo background checks and training on data security, confidentiality requirements when handling PII, and safeguarding of confidential UC information in accordance with 20 CFR Part 603. More detailed discussion of training is provided below. 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 various UI programs and processes. These roles are State Business Users, Regional/National DOL Business Users, and DOL or Vendor Technical Team Users.

- **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 that are documented in DOL procedures.

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.

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

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

  DOL UIRS users are 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 safeguarding UI information consistent with DOL's non-disclosure agreements with staff or contractor(s) using the system, which will include information on safeguarding confidential UC information and the acknowledgement requirements in 20 CFR Part 603. 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 training on privacy and safeguarding confidential information for all DOL staff and contractors who will be users of this system will be expanded to include information on protections of and safeguards for any data that constitutes confidential UC information and how such information must be maintained and stored to ensure compliance with the requirements of 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 data, including PII and confidential UC information, 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 accounts have system access and may only access the applications and data within the application to which they have been granted privileges. In addition, the system is monitored specifically for data exfiltration events.

  The system also incorporates comprehensive CRM tool audit logs. These audit logs meticulously track user actions within the application, such as login attempts, data access, and changes made to the data; no PII is accessed or viewed in the audit logs. This enables a detailed review of all user activities, helping to ensure accountability and detect any unauthorized or suspicious behavior by anyone accessing the system, whether State, DOL, or the Vendor Technical Team.

- **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. The Security Assessment and Authorization was last completed in May 2024.

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 Cloud Platform and the CRM Tool procured by DOL. 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 CRM Tool 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 a CRM Tool for data encryption at rest. The solution is also using DOL's Cloud Platform 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. In its current iteration, the UIRS relies upon states to select authorized State Business Users for UIRS. UIRS uses Active Directory and login authentication (i.e., multifactor authentication) to prevent unauthorized use of an authorized state user credential.
  DOL Business Users and DOL or Vendor Technical Team Users have verified their

identity 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 and contracted personnel who are given access to UIRS through Active Directory and login authentication (i.e., multifactor authentication) to prevent unauthorized use of an authorized DOL user credential.

11. PIA SIGNATURE PAGE

Reviewed by: Michelle Beebe, Administrator, Office of Unemployment Insurance, ETA Representative

Michelle Beebe Digitally signed by Michelle Beebe
Date: 2025.11.21 09:33:44 -05'00'

Signature

Reviewed by: Tim Erskine, Director of Enforcement, Benefits, and Payment Systems, OASAM-OCIO

TIMOTHY ERSKINE Digitally signed by TIMOTHY ERSKINE
Date: 2025.11.21 09:43:24 -05'00'

Signature

Reviewed by: Mara Blumenthal, DOL Privacy Office OASAM-OCIO

MARA BLUMENTHAL Digitally signed by MARA BLUMENTHAL
Date: 2025.11.21 08:48:03 -05'00'

Signature