New Hampshire Employment Security
www.nhes.nh.gov
"We're working to keep New Hampshire working"

GEORGE N. COPADIS, COMMISSIONER
RICHARD J. LAVERS, DEPUTY COMMISSIONER

ADMINISTRATIVE OFFICE
45 SOUTH FRUIT STREET
CONCORD, NH 03301-4857

CJG

SV

May 17, 2024

His Excellency, Governor Christopher T. Sununu
and the Honorable Council
State House
Concord, NH 03301

REQUESTED ACTION

To authorize New Hampshire Employment Security ("NHES") to enter into an Agreement with the United States Department of Labor ("USDOL") for utilization of Login.gov and associated resources in connection with the National ID Verification offering for a period of two years at no cost.

EXPLANATION

NHES seeks approval to enter into a Data Sharing Agreement (DSA) and Addendum A with USDOL, which provides for participation in its National ID Verification offering (Login.gov and USPS). This is part of an IT modernization effort, undertaken by USDOL and funded through the American Rescue Plan Act (ARPA), that is focused on updating and strengthening State Unemployment Compensation systems. Due to large-scale fraud perpetrated against many State systems in various ways during the pandemic, including through "claimants" with stolen identities trying to file for benefits or otherwise access such systems to commit fraud and theft, USDOL is making Login.gov available to the States to utilize for ID verification at no charge for a period of two years.

NHES has been seeking to implement a more robust and sustainable fraud detection system for those entering our New Hampshire Unemployment Insurance System ("NHUIS"). Currently being used by nine (9) other States and all of the Federal cabinet level agencies, Login.gov provides such a solution. NHES has been seeking this type of identity verification solution for quite some time and was not satisfied with proposals submitted in response to a prior competitive procurement. Past proposals from private entities would have required New Hampshire workers to provide Personally Identifiable Information (PII) to a private organization to verify their identity as a condition for being able to file for unemployment benefits. NHES was uncomfortable with such a scenario and jumped at the chance presented by Login.gov, as it allows NHES to utilize a proven, sophisticated identity verification solution to protect the unemployment program while making sure PII remains in the possession of federal agencies skilled in the storage and protection of sensitive information. For claimants who do not want to upload confidential information to

Login.gov from their computers or phones, there is a workaround which allows them to do their ID verification at a local U.S. Post Office of their choice.

NHES entered into a non-binding Data Sharing Agreement (DSA) with USDOL in April of 2023 to establish a foundation for participating in four federally funded IT modernization projects. The parties have now entered into a revised Data Sharing Agreement and Addendum A, which describes the National ID Verification offering (Login.gov and USPS) and the parties' respective obligations in detail. Login.gov provides protection by allowing for completion of robust identity verification before potentially fictitious claimants and employers are allowed into the system.

Submitted with the DSA and Addendum A is a State Technical Package, which describes the workings of the Login.gov and USPS program. The USDOL data breach notification plan is part of the agreement, but is a controlled document and has been redacted for security reasons.

New Hampshire Employment Security (NHES) has requested and obtained CIO approval of the revised DSA and Addendum A. In order to provide protection for our NHUIS system and ultimately to secure the safety and integrity of the Unemployment Insurance Trust Fund, we respectfully seek approval of this item.

Respectfully submitted,

Richard J. Lavers
Deputy Commissioner

STATE OF NEW HAMPSHIRE
DEPARTMENT OF INFORMATION TECHNOLOGY
27 Hazen Dr., Concord, NH 03301
Fax: 603-271-1516 TDD Access: 1-800-735-2964
www.nh.gov/doit

Denis Goulet
Commissioner

May 10, 2024

George N. Copadis, Commissioner
New Hampshire Employment Security
State of New Hampshire
45 S. Fruit Street
Concord, NH 03301

Dear Commissioner Copadis:

This letter represents formal notification that the Department of Information Technology (DoIT) has approved your agency's request to enter into a Memorandum of Understanding (MOU) with the US Department of Labor, as described below and referenced as DoIT No. 2024-136.

> The purpose of this request is to participate in a national IT modernization effort funded through the American Rescue Plan Act (ARP A), which is focused on updating and strengthening state Unemployment Compensation systems.

This is a no cost MOU, effective upon Governor and Council approval.

A copy of this letter must accompany New Hampshire Employment Security's submission to the Governor and Executive Council for approval.

Sincerely,

Denis Goulet

DG/jd
DoIT #2024-136

cc: Bill Laycock, IT Manager

New Hampshire Employment Security
www.nhes.nh.gov
"We're working to keep New Hampshire working"

GEORGE N. COPADIS, COMMISSIONER
RICHARD J. LAVERS, DEPUTY COMMISSIONER

ADMINISTRATIVE OFFICE
45 SOUTH FRUIT STREET
CONCORD, NH 03301-4857

May 10, 2024

Denis Goulet
Commissioner/CIO
Department of Information Technology
27 Hazen Drive
Concord, NH 03301

Dear Mr. Goulet:

REQUESTED ACTION AND EXPLANATION

New Hampshire Employment Security (NHES) requests CIO approval of this Memorandum of Understanding and Addendum A with the U.S. Department of Labor (USDOL) for participation in the **National ID Verification offering (Login.gov and USPS)**. This is part of a national IT modernization effort funded through the American Rescue Plan Act (ARPA), which is focused on updating and strengthening state Unemployment Compensation systems.

Due to large-scale fraud perpetrated in various ways during the pandemic, including through "claimants" with stolen identities trying to file for benefits or otherwise access state unemployment claims systems to commit fraud and theft, USDOL is making Login.gov available to the states to utilize for ID verification at no charge.

Although there is no charge for participation in the National Verification ID Offering, NHES felt it was important to submit the plan as part of the internal State review process with DoIT and the Attorney General's Office. If approved through Governor and Council, this Agreement will allow NHES to implement a more robust ID Verification process at no cost through USDOL for a period of two years.

PRIOR RELATED ACTIONS

NHES previously entered into a non-binding Memorandum of Understanding (MOU) with the U.S. Department of Labor (USDOL) dated April 26, 2024, concerning limited data sharing for projects funded by ARPA (Data Sharing Agreement or DSA). That MOU was supplemented by Addendum A, which provides the basis for participation in the Login.gov and USPS ID verification programs.

ALTERNATIVES AND BENEFITS

Not approving this Memorandum of Understanding with USDOL would prevent NHES from being able to participate in the National ID verification offering (Login.gov and USPS) at no cost. Given the lessons learned in the last several years, it is incumbent on NHES to have a robust identity verification system to keep the New Hampshire Unemployment Insurance System safe from fraud and, in so doing, to protect the integrity of the Unemployment Insurance Trust Fund. While there are private entities that provide similar services, those alternatives present other challenges to safeguarding the privacy of information exchanged in verifying the identity of claimants entering the system.

IMPACT ON OTHER STATE AGENCIES AND MUNICIPALITIES

If this agreement is not approved the NHES agency, state citizens and employers will be affected. This product is utilized by the Public, State of New Hampshire Employers and State Agencies. No financial impact or burden would be placed on any other state agencies or on the general fund.

CONTACT PERSONS:

William Laycock, IT Manager IV
603-228-4189
William.E.Laycock@doit.nh.gov

CERTIFICATION

The undersigned hereby certifies that the information provided in this document and any attachments is complete and accurate and that alternatives to the solution defined in this document have been appropriately considered.

Respectfully submitted,

George N. Copadis
Commissioner
NH Employment Security

DATA SHARING AGREEMENT
Between the
U.S. Department of Labor and
New Hampshire Employment Security
Concerning Disclosure of Information for
American Rescue Plan Act-Funded Activities

I. Parties to the Agreement

This data sharing agreement (Agreement) is between the U.S. Department of Labor (the Department) and New Hampshire Employment Security (state Unemployment Insurance (UI) agency) governing information that may be disclosed during the course of American Rescue Plan Act-funded activities, including, but not limited to, modernizing state IT solutions and Tiger Teams consultative assessments.

II. Background and Purpose of Agreement

Section 9032 of the American Rescue Plan Act (ARPA) (Public Law 117-2) creates a new Section 2118 of the CARES Act and provides an appropriation to the Secretary of Labor to: 1) detect and prevent fraud, 2) promote equitable access, and 3) ensure timely payment of benefits to eligible workers with respect to unemployment compensation (UC) programs (collectively, the ARPA Goals).

The Department has identified initiatives to support these ARPA Goals, including activities such as modernizing State UI systems and Tiger Team Consultative Assessments[1]. The Department may use agent(s) or contractor(s) to perform some or all of these services, including implementation of solutions.

Modernizing State UI Systems

One initiative of this plan is to develop solutions to modernize states' legacy systems and technology. If the Department and the state UI agency agree to partner to implement solutions to modernize state UI systems, they will develop, enter into, and attach an addendum to this Agreement that describes the roles and responsibilities of that partnership in detail.

Facilitating Tiger Teams Consultative Assessments

The Tiger Teams will work with states to identify areas to enhance their existing efforts towards achieving the ARPA Goals and make actionable recommendations for the states to

[1] The Department is supporting states with improving UC systems and processes that achieve the following goals: 1) preventing, detecting, and recovering funds from fraud; 2) promoting equitable access; and 3) ensuring the timely payment of benefits as well as activities to reduce workload backlogs, for all UC programs. This support may include a consultative assessment of their UC program, wherein the Department will leverage a multi-disciplinary team of experts (i.e., Tiger Teams) designed specifically to analyze state UC systems and process challenges. UIPL No. 02-22

implement. Based on this review, the Tiger Team will recommend solutions to the state that may include activities such as workflow adjustments, process improvements, technology updates, and/or communication revisions. The Department and the state UI agency will negotiate which of these recommendations to implement. If the Department and the state UI agency agree to partner to implement certain recommendations, they will develop and attach an addendum to this Agreement that will describe the roles, responsibilities, and expectations of that partnership.

Supporting Data Sharing Protections

As part of the Department's efforts towards modernizing state IT solutions and conducting the Tiger Teams assessments, the state UI agency may share Confidential UC Information and Sensitive Information (both terms defined below) to members of a Department project team, their agents, and contractors. In the event the parties determine that it is necessary for the state UI agency to disclose specific Confidential UC Information or Sensitive Information to the Department, or its agent(s) or contractor(s), for purposes of conducting the initiatives or as otherwise set forth herein, the parties will identify that information in an addendum and attach the addendum to this Agreement. The parties agree to add any additional provisions necessary to such addendum in order to fully comply with the requirements of 20 C.F.R. 603.9 and 603.10.

Regardless of the parties' efforts to document the specific Confidential UC Information and Sensitive Information that may be identified for disclosure in an addendum to this Agreement, the parties acknowledge that for purposes of complying with federal and state law, this Agreement shall apply to and govern the incidental disclosure and receipt of Confidential UC information and Sensitive Information in connection with any initiatives and work contemplated herein.

The Department and state UI agency shall add addenda to this Agreement as appropriate to address additional technical details, describe scopes of work, identify which initiatives the parties will participate in, or for any other reason as agreed by the parties. All addenda to this Agreement shall be in writing and signed by the parties.

III. Definitions of "Confidential UC Information" and "Sensitive Information" that May Be Disclosed by the State UI Agency

A. "Confidential UC Information" includes any UC information which reveals the name or any identifying particular about any individual or any past or present employer or employing unit, or which could foreseeably be combined with other publicly available information to reveal any such particulars (individual's name, phone numbers, Social Security numbers, benefits received, taxes paid, etc.). *See* 20 C.F.R. Part 603.

B. "Sensitive Information" generally includes information about the operations of the state UI agency, whether in oral and/or written form, obtained from the state UI agency during discussions or communications with the Department and its agents(s) or contractor(s). Information may include, but is not limited to, information concerning

the state UI agency's computer systems, staff, telephone numbers, any and all processes, current and future architectures (including hardware, middleware, software, networks, etc.), source code, passwords, security architecture, security processes and management, security audits, intellectual property, current services, services not yet publicly announced, state UI agency's strategic plans, and so forth.

IV. Purpose of this Agreement and Legal Authority

A. The purpose of this Agreement is:

1. To comply with requirements related to Confidential UC Information -

   a. Specifically, to comply with 20 C.F.R Part 603, including 20 C.F.R. 603.10(a)(2), which requires a state agency disclosing Confidential UC Information to a public official or an agent or contractor of a public official to enter into an agreement with the public official; and

   b. To provide the state UI agency with assurances that the Department and its agent(s) or contractor(s) will comply with all the applicable requirements of 20 C.F.R. Part 603 regarding data security and confidentiality.

2. To provide the state UI agency with assurances that the Department, and its agent(s) or contractor(s), will take measures (as specified in Sections VII and VIII below) to protect Sensitive Information received as part of its engagement in modernizing state IT solutions and Tiger Teams consultative assessments, except as required by federal law or regulations.

B. Legal Authority

1. Section 303(a)(1) [42 U.S.C. 503(a)(1)] of the Social Security Act;

2. 20 C.F.R. Part 603;

3. Section 2118 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act (Pub. L. 116-136), as amended; and

4. New Hampshire Revised Statutes RSA 282-A:118, III and IV.

V. General Provisions

A. Nothing in this Agreement shall be interpreted as limiting, superseding, or otherwise affecting either the Department's normal operations or its decisions in carrying out its statutory or regulatory duties. This Agreement does not limit or restrict the Department from participating in similar activities or arrangements with other entities.

B. Nothing in this Agreement shall be interpreted as limiting, superseding, or otherwise affecting either state UI agency operations or decisions in carrying out its statutory or regulatory duties. This Agreement does not limit or restrict the state UI agency from participating in similar activities or arrangements with other entities.

C. This Agreement will be effective upon signature and will terminate one (1) year after signature, with the option for the parties to extend this date by written agreement signed by the parties. Any party to the Agreement may terminate this Agreement by providing fifteen (15) days' notice of their intent to terminate the Agreement.

D. This Agreement does not commit or obligate funds. The parties are therefore responsible for their own costs, if any, incident to or arising out of this Agreement.

E. Nothing in this Agreement is intended to constitute a waiver of Federal sovereign immunity.

F. Nothing in this Agreement is intended to constitute a waiver of State sovereign immunity.

VI. Provisions Specific to Confidential UC Information

A. The Department or its agent(s) or contractor(s) will not redisclose Confidential UC Information that may be received as part of the IT modernization project or consultative assessment, except as required by federal law or regulation. The state UI agency agrees that in the event a state participates in an ARPA-funded initiative contemplated under this Agreement, Department project teams, their agents and contractors, and Department regional office personnel working on that initiative or other ARPA-funded initiatives may access Confidential UC information received from the state UI agency for all of the following purposes:

- evaluating the outcome and success of an initiative;
- conducting evidence-based research and analysis regarding the effectiveness, outcomes, and equitable application of initiatives in supporting the ARPA Goals;
- assisting a Department project team or state UI agency when considering potential participation in another ARPA initiative; and
- implementing and supporting the state UI agency with any initiative contemplated herein.

B. If the Department or its agent(s) or contractor(s) fails to comply with any provision of this Agreement, the state UI agency must take action, in accordance with 20 CFR 603.10(c).

C. To the extent practicable, the Department will mitigate any harmful effect on individuals whose information (from a state) was breached in an incident for which the Department or its agent(s) or contractor(s) were responsible.

VII. Provision Specific to Sensitive Information

A. The Department or its agent(s) or contractor(s) will not redisclose Sensitive Information that may be received as part of the IT modernization project or consultative assessment without explicit approval from the state UI agency, except as required by federal law or regulation. The state UI agency agrees, however, that in the event a state participates in an ARPA-funded initiative contemplated under this Agreement, Department project teams, their agents and contractors, and Department regional office personnel working on that initiative or other ARPA-funded initiatives, may access Sensitive Information received from the state UI agency for all of the following purposes:

- evaluating the outcome and success of an initiative;
- conducting evidence-based research and analysis regarding the effectiveness, outcomes, and equitable application of initiatives in supporting the ARPA Goals;
- assisting a Department project team or state UI agency when considering potential participation in another ARPA initiative; and
- implementing and supporting the state UI agency with any initiative contemplated herein.

VIII. Data Security and Confidentiality

A. The Department provides assurance that the Department and its agent(s) or contractor(s) will abide by the terms of this Agreement. The Department and its agent(s) or contractor(s) are required to safeguard Confidential UC Information, as required by 20 CFR 603.9, against unauthorized access, re-disclosure, or both. The Department specifically assures the state UI agency that the Department and its agent(s) or contractor(s) will, in regard to all information:

1. Use the information only for the specific purpose permitted in this Agreement, and not re-disclose the information for any other purpose, except as expressly provided in this Agreement or as required by law. If the Department receives a Freedom of Information Act (FOIA) request for information disclosed during the state's participation in modernizing IT solutions, Tiger Teams consultative assessments, or Tiger Team project implementation project(s), the Department will seek to protect information to the extent permitted under any applicable FOIA exemptions, including the exemption on disclosing information that would result in an unwarranted invasion of personal privacy and the exemption that protects various types of law-enforcement information. See 5 U.S.C. 552(b).

2. Store the information in a place physically secure from access by unauthorized persons.

3. Store and process the information in an electronic format that is secure from access by unauthorized persons.

4. Take precautions to ensure that only authorized personnel have access to computer systems in which the information is stored.

5. Information will be made available only to those staff of the Department or its agent(s) or contractor(s) who require the information to carry out the responsibilities described in this Agreement.

6. Instruct all project staff with access to the information on the confidentiality requirements of this Agreement, the applicable federal and state confidentiality requirements, and the sanctions specified by state law for unauthorized disclosure of information.

7. Sign an acknowledgment that all personnel having access to the disclosed information have been instructed in accordance with Article VIII.A.6 of this Agreement, will adhere to the state UI agency's confidentiality requirements which are consistent with subpart B of 20 CFR part 603, and will report any infraction of these rules to the state UI agency promptly.

8. Transmit the information by a secure method and encrypt all personally identifiable information (PII) during receipt, transmission, storage, maintenance, and use.

9. Notify the state UI agency of any breach of security or system changes (hardware or software).

10. Destroy the information, according to procedures, if any, specified by the state UI agency, when the engagement is completed and provide confirmation in writing to the state that this has successfully been accomplished.

11. Maintain a system sufficient to allow an audit of compliance with these safeguard provisions.

12. Allow the state UI agency access for on-site inspections to ensure that the requirements of the State's law and this Agreement are met. Inspections for these purposes shall not be limited by the Department or its agent(s) or contractor(s).

13. Adhere to subsequent Departmental and State guidelines on information handling during all phases of the project.

IX. Contact Persons/Authorized Officials

A. The primary contact/s at New Hampshire Employment Security for all matters related to the fulfillment of this Agreement is/are:

Michael Burke
45 South Fruit Street
Concord, NH 03301
603-447-1463
Michael.H.Burke@nhes.nh.gov

B. The primary contact/s at the Department for all matters related to the fulfillment of this Agreement is/are:

In General:

Michelle Beebe
200 Constitution Avenue NW
Washington, DC 20210
202-693-3029
Beebe.Michelle.E@dol.gov

X. Signatures

The signatories below agree to the terms and conditions of this Agreement on behalf of the parties to this Agreement.

U.S. Department of Labor

Carolyn Angus-Hornbuckle

Digitally signed by Carolyn Angus-Hornbuckle
Date: 2024.04.22 09:41:39 -04'00'

Carolyn Angus-Hornbuckle — Date
Assistant Secretary for Administration and Management

New Hampshire Employment Security

George N.Copadis

Digitally signed by George N.Copadis
Date: 2024.04.22 15:42:22 -04'00'

George N. Copadis — Date
Commissioner

New Hampshire Department of Justice

Duncan A. Edgar

Digitally signed by Duncan A. Edgar
Date: 2024.04.26 14:58:25 -04'00'

Duncan Edgar — Date
Assistant Attorney General

ADDENDUM A
to the
DATA SHARING AGREEMENT
Between the
U.S. Department of Labor
and
New Hampshire Employment Security
Concerning Disclosure of Information for
American Rescue Plan Act-Funded Activities for the

National Identification (ID) Verification Offering

I. Overview

This is an addendum to the Data Sharing Agreement between the U.S. Department of Labor (Department) and New Hampshire Employment Security (state Unemployment Insurance (UI) agency) Concerning Disclosure of Information for American Rescue Plan Act-Funded Activities dated April 26, 2024 (Data Sharing Agreement).

II. Background and Purpose of Addendum

This Addendum to the Data Sharing Agreement provides solely for the roles, responsibilities, timeline and intended outcomes for the National ID Verification Offering. The National ID Verification Offering includes Department-sponsored, government-operated ID verification systems that offer online verification services through partnership with the U.S. General Services Administration's (GSA) Login.gov and in-person verification services through partnership with the U.S. Postal Service (USPS).

III. Scope of Work for this National Identification ID Verification Offering

This section describes the scope of work for the National ID Verification Offering for both the GSA Login.gov and USPS in-person proofing programs.

The National ID Verification Offering is designed to: (1) provide identity proofing on the initial UI claim process; and (2) allow a state UI agency to timely receive this data to process claims.

The core functionality of the National ID Verification Offering is identity verification. While the National ID Verification Offering will inform processing of claims, it will not include development of information technology applications or features for the state UI agency employees' use in determining eligibility or adjudicating claims and appeals. The state UI agency will continue to make determinations as to the validity of the individual, the completeness of the claim, and the eligibility of the individual. Additional features may be addressed by future enhancements.

IV. Roles and Responsibilities for the National ID Verification Offering

A. As a condition to participating in one or both programs in the National ID Verification Offering, the state UI agency agrees to do the following:

1. Report Individual-Level Data: Starting in May 2024 and quarterly thereafter, provide the following data points for each individual who is referred for identity verification to one or both programs on an individual level basis, in a format to be agreed upon between the state UI agency and the Department.

   Note: All individuals referred to the National ID Verification Offering service(s) should be reported in the quarter in which referred by the State. If an individual completes a service in the following quarter (e.g., referral to the service occurs on Sept. 30th and verification is completed on October 3rd), then the state should also report this individual in the subsequent quarterly submission, including the updated verification result, using the same State Specific Unique Identifier in each case.

   a. State-provided Elements

      i. State Specific Unique Identifier (not SSN): This is the state-assigned unique identifier that follows individual claimants through the ID verification process, and serves as a linking variable across all elements shared with the Department;
      ii. Date of Referral by State;
      iii. Zip;
      iv. Gender;
      v. Age;
      vi. Race;
      vii. Ethnicity;
      viii. Education Level;
      ix. Industry;
      x. Occupation;
      xi. Disability (if identified); and
      xii. Language Preference.

   b. Login.gov: The state agrees to match the data elements in IV.A.1.a with the following data elements received back from the Department, where applicable. Note that these elements will be returned only for individuals who reach IAL1 or ID verified status.

      i. State Specific Unique Identifier (swa_xid): This is the state-assigned unique identifier that follows individual claimants through the ID verification process, and serves as a linking variable for state-provided elements. This is the same number as provided in IV.A.1.a.i and IV.A.1.c.i.

ii. Status (identity_assurance_level): This provides the level at which the individual completed ID assurance (IAL1 or ID verified).

c. USPS: The state agrees to match the data elements in IV.A.1.a with the following data elements received back from the Department, where applicable.
   i. State Specific Unique Identifier (swa_xid): This is the state-assigned unique identifier that follows individual claimants through the ID verification process, and serves as a linking variable for state-provided elements. This is the same number as provided in IV.A.1.a.i and IV.A.1.b.i.
   ii. Proofing Post Office (proofing_post_office): The ID number for the post office that performed the transaction.
   iii. Primary ID Type (primary_id_type): A description of the ID that was presented during the transaction.
   iv. Secondary ID Type (secondary_id_type): A description of the secondary ID that was presented during the transaction.
   v. Passed with Suspicion (fraud_suspected): Customer passed with suspicion (True or False).
   vi. Status (status): In-person passed; in-person failed; in-person expired; in-person absented; or in-person not-exist.

State's initial submission must include all quarters since the beginning of the state's participation in the National ID Verification Offering. If a state UI agency is unable to provide the data points by the deadline, the state UI agency may request an extension of time in writing to comply with this provision. To request an extension, the state UI agency may contact their ETA Regional Office.

The state agrees to provide the Department with appropriate context, including any supporting documentation that might be needed, to interpret or analyze the data. This information will be used by the Department to assess the effectiveness and equity of ID verification as set forth in UIPL No. 11-23, Section 4.c.

2. Continue operating the state UI agency's existing UI system, in accordance with federal and state law, regulations, and guidance.
3. Assign a state UI agency staff member with decision-making authority for the state UI agency.
4. Assign a state UI agency staff member responsible for day-to-day operations who will be available, as needed, to respond to issues that arise.
5. Provide appropriate additional IT staff support to maintain functionality.
6. Provide the Department direct access to the state UI agency senior stakeholders across appropriate state UI agency components, as well as state UI agency staff who are knowledgeable in UI claims processing.
7. Provide the Department with necessary state UI agency credentials, building and systems access on a case by case basis, without reservation, (in adherence to the safeguards described in the Data Sharing Agreement (DSA)), and IT resources.

8. Provide the Department with access to necessary information related to the work the Department will perform, to include all relevant project materials, internal meetings, standard operating procedures, and other resources.
9. Collect sufficient information from individuals to facilitate ID verification and to comply with UIPL No. 16-21, and future guidance published by ETA, for any individual that does not complete ID verification or fails ID verification.
    a. If the Department or state UI agency identifies any ID verification compliance issues related to participation in the National ID Verification Offering before, during, or after the implementation of one, or both, programs in the National ID Verification Offering, the state will:
        i. Work in partnership with the Department to identify options to become compliant;
        ii. Meet ID verification compliance with current and future relevant guidance within 12 months of this executed Addendum or on a timeline agreed upon between the Department and the state; and
        iii. Maintain an open line of communication with the Department regarding potential barriers to becoming compliant and/or challenges encountered/positive practices implemented as a result of becoming compliant.
10. If the state chooses to participate in the more in-depth analysis as described in Section 4.c.iii.C. of UIPL No. 11-23, disclose additional individual-level data to the Department for purposes of assessing the effectiveness of ID verification.
11. Provide feedback on the effectiveness of the experience, which may include collecting and sharing relevant program metrics and responding through surveys.
12. For any materials that the state chooses to publish on their website, ensure that confidential unemployment compensation (UC) information is redacted.
13. Use of one or both of the National ID Verification Offering products does not alter the state's obligation to employ merit staffing principles throughout the claim cycle for eligibility determinations, including processing claims that originate through participation with this offering and support individuals applying for and/or receiving UC, making any necessary adjustments to existing systems and processes, as set forth in Section 303(a)(1) of the Social Security Act and related Department guidance.

B. In connection with either service described in the National ID Verification Offering, the Department agrees to:

1. As necessary, maintain responsibility for communication with National ID Verification Offering stakeholders, including but not limited to the state, GSA, and USPS.
2. Provide government-operated ID verification systems to states that support online verification services through partnership with GSA's Login.gov and in-person

verification services through partnership with USPS, subject to the availability of funding and necessary agreements being in place.

3. Support the state UI agency to set priorities, resolve issues, and ensure the design and delivery of digital services to the state UI agency and the individuals it serves.
4. Support and promote the use of agile methodologies and modern technology infrastructure to deliver the scope of the offering.
5. Give advice and technical assistance to the state UI agency on digital service solutions, information technology needs, business processes, and policy.
6. Notify the state of any compliance issues identified related to participation in the National ID Verification Offering, including sufficient detail documenting the issue(s).
   a. Collaborate with the state UI agency to assist in compliance as the project nears its deployment date and continue to serve as a strategic partner and collaborator in ensuring the state UI agency takes the necessary actions to meet the documentation requirements detailed in UIPL No. 16-21 and future guidance published by ETA.
7. Assist and conduct research with state UI agency customers and internal users to evaluate the offering and to determine how the services can be improved.
8. As necessary, coordinate IT program activities with stakeholders endeavoring to achieve seamless integration of program elements with ongoing policy, leadership, and service delivery operations.

V. Roles and Responsibilities Specific to Participation in the USPS In-Person Proofing Program

As a condition of participating in the USPS in-person proofing program, the state UI agency and Department agree to do the following:

A. The state UI agency shall:

1. Grant the Department the authority to facilitate identity proofing through the USPS In-Person Proofing process on behalf of the state UI agency and affirm that this project does not violate state law.
2. Acknowledge that the Department has issued a Federal Register notice explaining its determination that the USPS has adequate safeguards in place to satisfy the confidentiality requirements of Section 303(a)(1) of the Social Security Act and as such, the requirements of 20 C.F.R. 603.9 do not apply to disclosures of confidential UC information to the USPS under this project.
3. Provide the initial point of contact for UC claimants for customer service inquiries related to the USPS In-Person Proofing process. The state UI agency will be responsible for handling basic customer inquiries and troubleshooting simple issues.
4. Provide UC Claimants with all information and instructions necessary to complete the USPS In-Person Proofing process. Development and creation of these materials will be with the assistance and consultation of the Department.

5. Provide staff resources to test the implementation of the USPS In-Person Proofing process before public launch, which may include both system integration testing and in-person testing at the USPS retail locations.
6. Provide sufficient location data to determine the potential USPS retail locations for the National ID Verification Offering and review and agree to the locations once those locations are identified by the Department and USPS.
7. Maintain and make available, upon a reasonable request, records relevant to the USPS In-Person Proofing process.
8. Provide a state-specific claimant unique identifier to the Department for the purposes of facilitating the USPS In-Person Proofing process.
9. Report any loss, theft, or unauthorized access to, or disclosure of data related to USPS In-Person Proofing from the state UI agency's system to the DOL Incident Response Team within 1 hour or as soon as possible after any security breach is discovered.
10. Promptly remove from the state UI agency's system the ability for a claimant to opt-in to the USPS In-Person Proofing process, after notice from the Department that the agreement between the Department and the USPS is terminated.
11. Obtain the Department's express written consent, or (when time is of the essence) consent via a phone call with subsequent e-mail confirmation of approval, before distributing or otherwise publishing a press release or similar public announcement regarding the USPS In-Person Proofing or the relationship between the Department and the state UI agency in relation to this addendum. Furthermore, state UI agency will not display, use or otherwise publish the Department's trademarks, trade dress, and materials subject to copyright protection without the Department's prior written consent to the specific use, display, or publication.
    a. Notwithstanding the foregoing, (1) state UI agency may make disclosures without the other party's consent as required by law or as required or requested by any Federal, regulatory, state, or local governmental body in the proper exercise of its oversight or investigatory jurisdiction, (2) state UI agency may reference and describe the USPS In-Person Proofing in routine public statements as well as in marketing materials without providing advance notice to the Department or obtaining its consent, and (3) the Department may reference and describe this National ID Verification Offering in routine public statements as well as in marketing materials without providing advance notice to state UI agency or obtaining its consent.

B. The Department shall:

1. Enter into an agreement with the USPS to provide in-person identity proofing services to the state UI agency, utilizing the USPS In-Person Proofing process.
2. Facilitate the testing of the USPS In-Person Proofing process before public launch, which may include both system integration testing and in-person testing at the USPS retail locations.
3. Facilitate the secure transmission of a Department-generated enrollment code to the USPS to allow a claimant to use the USPS In-Person Proofing process.

a. The enrollment code allows USPS to access a claimant's full name, address, and e-mail address which the Department collects from the claimant.

4. Provide escalated point of contact for technical customer services inquiries related to the USPS In-Person Proofing process. The Department will be responsible for troubleshooting issues or coordinating with USPS to troubleshoot issues related to USPS In-Person Proofing and state UI agency system integration.
5. In the event of a loss, theft, or unauthorized access to or disclosure of data related to USPS In-Person Proofing, the Department will report that breach to the state UI agency as soon as possible after the security breach is reported to the Department.
6. As necessary, maintain responsibility for communication and outreach with appropriate stakeholders.
7. Obtain the state UI agency's express written consent, or, when time is of the essence, via a phone call with subsequent e-mail approval, before distributing or otherwise publishing a press release or similar public announcement regarding the USPS In-Person Proofing National ID Verification Offering or the relationship between the Department and the state UI agency in relation to this addendum. Furthermore, the Department will not display, use, or otherwise publish the state UI agency's trademarks, trade dress, and materials subject to copyright protection without the state UI agency's prior written consent to the specific use, display, or publication.
    a. Notwithstanding the foregoing, (1) the Department may make disclosures without the other party's consent as required by law or as required or requested by any Federal, regulatory, state, or local governmental body in the proper exercise of its oversight or investigatory jurisdiction, (2) the Department may reference and describe the USPS In-Person Proofing in routine public statements as well as in marketing materials without providing advance notice to the state UI agency or obtaining its consent, and (3) the state UI agency may reference and describe this National ID Verification Offering in routine public statements as well as in marketing materials without providing advance notice to the Department or obtaining its consent.

VI. Other Provisions

This Addendum will be effective as of the date of the last signature below and will terminate on the expiration date of the Data Sharing Agreement to which it is attached, with the option for the parties to extend this date if the Data Sharing Agreement is extended and with written notice. The state UI agency or the Department may terminate this Addendum at any time by providing at least thirty (30) calendar days advance written notice to the other party.

If the state UI agency decides to participate in the additional research opportunity described in UIPL No. 11-23, Section 4.c.iii.C., the parties will enter into an additional addendum to establish the roles and responsibilities of the parties and attach it to the Data Sharing Agreement.

By signing this Addendum, the state UI agency agrees that all work products developed as a result of the work described in this Addendum, if applicable, may be published by the Department as a public resource for other states to utilize, at the Department's discretion. The state UI agency will be responsible for redacting any confidential UC information and sensitive information before publication.

VII. Contact Persons/Authorized Officials

A. The primary contact at New Hampshire Employment Security for all matters related to the fulfillment of this Addendum is:

Michael Burke
45 South Fruit Street
Concord, NH 03301
603-447-1463
Michael.H.Burke@nhes.nh.gov

B. The primary contact at the Department for all matters related to the fulfillment of this Addendum is:

Michelle Beebe
200 Constitution Avenue NW
Washington, DC 20210
202-693-3458
Beebe.michelle.e@dol.gov

VIII. Signatures

The signatories below agree to the terms and conditions of this Addendum on behalf of the parties to this Addendum.

U.S. Department of Labor

Carolyn Angus-Hornbuckle

Digitally signed by Carolyn Angus-Hornbuckle
Date: 2024.05.01 16:49:04 -04'00'

Carolyn Angus-Hornbuckle Date
Assistant Secretary for Administration and Management

New Hampshire Employment Security

George N.Copadis

Digitally signed by George N.Copadis
Date: 2024.05.07 12:58:03 -04'00'

George N. Copadis Date
Commissioner

New Hampshire Department of Justice

Duncan A. Edgar

Digitally signed by Duncan A. Edgar
Date: 2024.05.17 13:21:12 -04'00'

Duncan Edgar Date
Assistant Attorney General

New Hampshire Governor & Executive Council

Date

Exhibit #1

IDENTITY VERIFICATION- NATIONAL OFFERING

State Workforce Agency Technology Handout

Office of the Chief Information Officer
PART OF THE OASAM TEAM

This package is designed to provide State Workforce Agencies (SWA) with technical information regarding the level of effort required for a state partner to participate in in the USDOL ID Verification National Offering.

Level of Effort

Each SWA will make the determination as to which offering is chosen to support Identity Verification for their state claimant population. The technological lift to support that implementation is dependent on two main factors. The existing technological infrastructure flexibility and the options chosen by the state for implementation. USDOL technical implementation is planned to be completed in a six-week period. This schedule is completely dependent on the state partner's ability to support, therefor deviations are permissible in the event a state can not support the below implementation schedule.

- Sprint 1 – 2 weeks – Design of state specific web pages.
- Sprint 2 – 2 weeks – Engineering of specified design in previous sprint
- Sprint 3 – 2 weeks – Testing the integration and content with USDOL and state partners.

Technical Help Desk

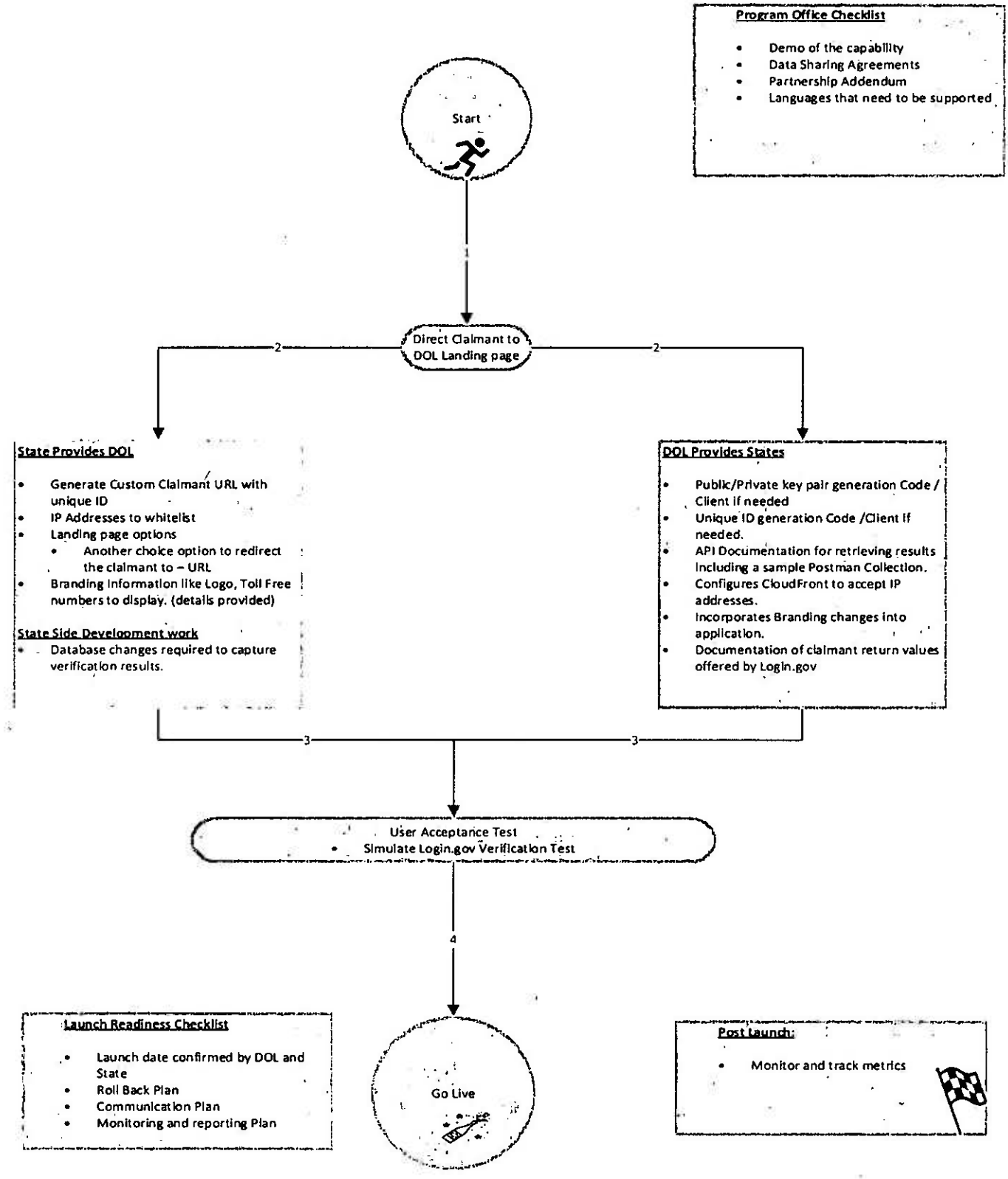
USDOL's Office of Chief Information Officer (OCIO) maintains the UI Claimant Portal Helpdesk to support all SWA partners participating in the National offering. States will be asked to provide a minimum of two points of contacts. The POCs should ensure that the ui-claimant-portal-helpdesk@dol.gov email address is added to their contacts to ensure that emails are not redirected to a spam or junk folder.

- Eash state needs to identify at a minimum of 2 POCs for technical notifications. The State POCs will receive notifications each time USDOL releases, any changes to the service and any service outages from either USDOL or our federal partners.
- States will also submit any technical issues, systematic changes on the state side or outage issues to the ui-claimant-portal-helpdesk@dol.gov email address.

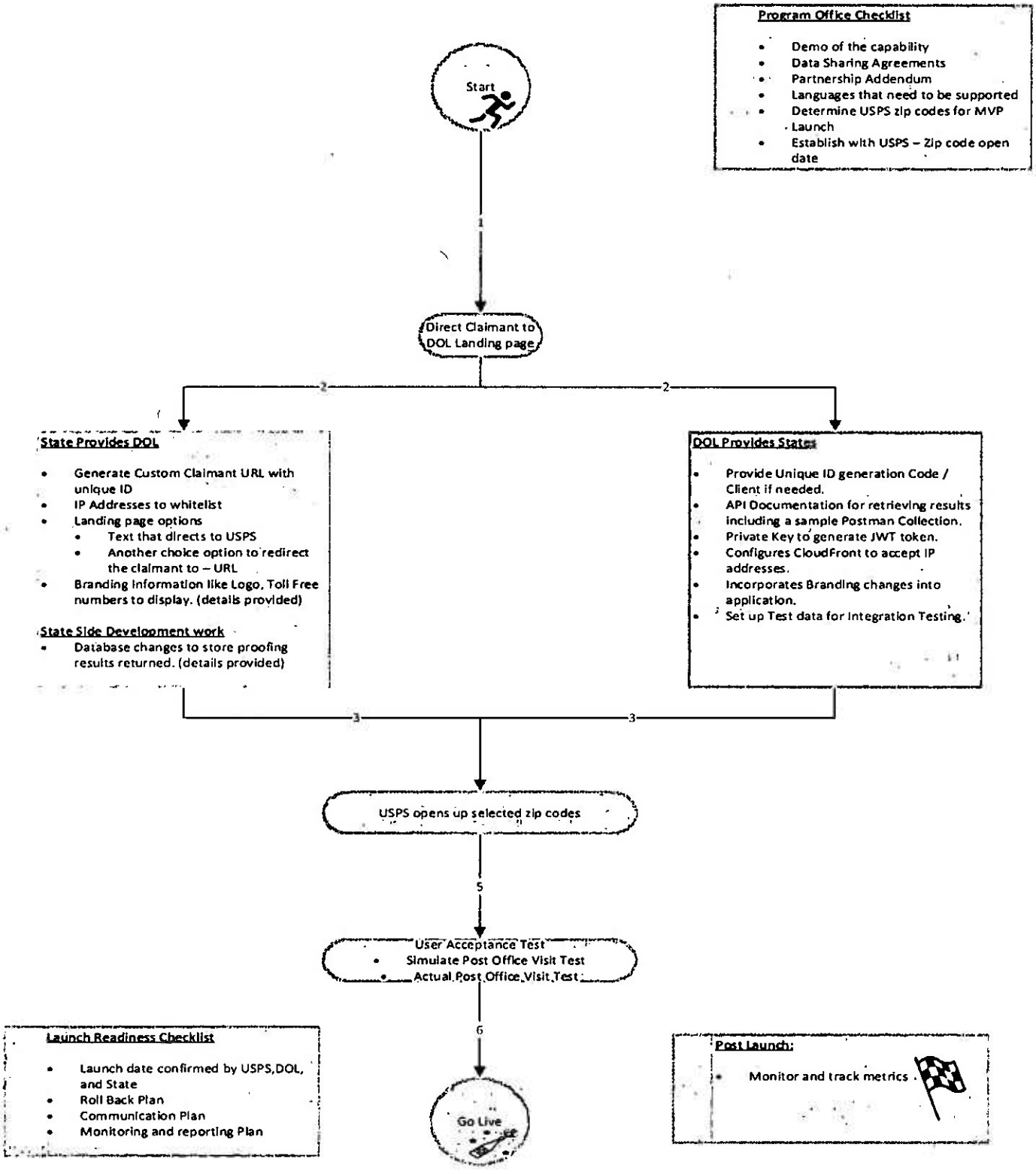
Attachments

- Attachment 1 – Workflow and information needed from states for login.gov designs.
- Attachment 2 – Workflow and information needed from states for USPS designs.
- Attachment 3 – Data Elements State will need to program into their system to capture results returned from login.gov.
- Attachment 4 – Data Elements State will need to program into their system to capture results returned from USPS for IPP.
- Attachment 5 – API call requirements for USPS results.
- Attachment 6 – API call requirements for Login.gov results.

Attachment 1 – Workflow and information needed from states for login.gov designs.



Attachment 2 – Workflow and information needed from states for USPS designs.



Attachment 3 – Data Elements State will need to program into their system to capture results returned from login.gov.

Name	Example Value	Description	Type/Format
id	19c05261-db64-4c78-ad54-4e1a75fdc508	The claimant's unique DOL provided identifier	Type: String Format: UUID
swa_xid	20230727-141053-1234567-123456789	The claimant's unique state provided identifier	Type: String
claimant_id	b2d2d115-1d7e-4579-b9d6-f8e84f4f56ca	The claimant's unique login.gov provided identifier	Type: String
identity_provider	login.gov	The identity assurance provider	Type: String
identity_assurance_level	2	The level at which the claimant has completed identity assurance.	Type: Integer
validated_at	2022-02-26T14:47:02-06:00	Datetime of the last time the claimant was validated by the DOL	Type: String Format: Datetime
swa_code	XX	2-letter code identifying the State Workforce Agency	Type: String
email	test@example.com	The claimant's email	Type: String Max Length: 128 characters
all_emails	["test@example.com", "test2@example.com"]	A list of all email's associated with the claimant's Login.gov account	Type: Array
first_name	Some	The claimant's given name	Type: String
last_name	One	The claimant's family name	Type: String
birthdate	2000-01-01	The claimant's date of birth	Type: String Format: Date
ssn	900-00-1234	The claimant's social security number	Type: String Pattern: ^[0-9]{3}-[0-9]{2}-[0-9]{4}$

address	{
	"address1": "123 Any St",
	"city": "Somewhere",
	"state": "XX",
	"zipcode": "12345"
	}
		The claimant's address	Type: Object

address 1	123 Any St	Subset of address. The claimant's first address	Type: String Max Length: 64 characters
city	Somewhere	Subset of address. The claimant's city	Type: String Max Length: 64 characters
state	XX	Subset of address. The claimant's state	Type: String Min/Max Length: 2 characters
zipcode	12345	Subset of address. The claimant's zipcode	Type: String Max Length: 12 characters Pattern: ^\\d{5}(-\\d{4})?$
phone	555-555-1234	The claimant's phone number	Type: String
verified_at	2022-02-03T09:06:36-06:00	Datetime of the last time the claimant was validated by the DOL	Type: String Format: Datetime

Attachment 4 – Data Elements State will need to program into their system to capture results returned from USPS for IPP.

Unset fields are omitted from the response.

Field	Description	Type/Format
swa_xid	The unique identifier shared between the state and DOL	33 Character String
error_message	If an error occurred, a description of the error	String
records	Contains the list of enrollment codes and supporting information associated with the swa_xid	Array
enrollment_code	The code used at USPS	Numeric String
first_name	The claimant's first name.	String
last_name	The claimant's last name.	String
street_address	The claimant's street address.	String
city	The claimant's city.	String
state	The claimaint's state:	2 letter abbreviation
zip_code	The claimant's zip code	String
email_address	The claimant's email address	String
expiration_date	A DOL configured number of days after the enrollment has started. Note: this isn't used since USPS doesn't accept a configurable expiration.	Date
status	Passed: The claimant completed the proofing transaction successfully.	"In-person passed",
	Failed: The claimant completed the proofing transaction unsuccessfully.	"In-person failed",
	Expired: The enrollment code has expired	"In-person expired",
	Absented: The enrollment has not expired, and the claimant has not completed enrollment.	"In-person absented",
	Not-exist: The enrollment code exists in the USDOL system but does not exist in the USPS system. NOTE: This status is an edge case and would not expect to be returned.	"In-person not-exist"
failure_reason	A description of why the customer failed in-person proofing.	String
proofing_post_office	The name of the post office that performed the transaction.	String
proofing_city	The city of the post office that performed the transaction.	String
proofing_state	The state of the post office that performed the transaction.	2 letter abbreviation
primary_id_type	A description of the ID that was presented during the transaction.	String
secondary_id_type	If present, a description of the secondary ID that was presented during the transaction.	String

transaction_start_date_time	The date and time that the in-person proofing transaction started. Note: this is a pass-through from USPS and appears to have a bug in the time.	Date and time*
transaction_end_date_time	The date and time that the in-person proofing transaction ended. Note: this is a pass-through from USPS and appears to have a bug in the time.	Date and time*
fraud_suspected	An indication of whether fraud was suspected by the Postal Clerk	"True" or "False"
proofing_confirmation_number	A confirmation number for the in-person proofing event. Generated by USPS.	String
response_message	Response message from USPS indicating the results of the call to get proofing results.	String
time_created	When the record was recorded in the DOL system.	Date and time with timezone
time_updated	When the record was last updated in the DOL system.	Date and time with timezone
time_email_sent	Date and time DOL sent an email to the claimant. Only applies to states using DOL frontend.	Date and time with timezone
time_email_reminder_sent	Date and time DOL sent an email reminder to the claimant. Only applies to states using DOL frontend.	Date and time with timezone

USPS IN PERSON PROOFING: ENDPOINT DEFINITION AND USAGE

Version 0.4
7/26/2023

DOCUMENT IDENTIFICATION INFORMATION	
Version:	0.4
Date Created:	4/17/2023
Created By:	Joshua Axtell
Date Published:	DRAFT

Change History			
Version	**Date**	**Description**	**Author**
0.2	4/19/2023	Removed unreferenced endpoints. Updated flow diagrams. Added result endpoint	Joshua Axtell
0.3	6/27/2023	The section related to directly connecting to the USPS end point has been removed.	Preethi Sudhakar
0.4	7/26/2023	Updated to more accurately reflect the current offering	Joshua Axtell
0.5	11/29/2023	Updated description indicating limits of swa_xid	Joshua Axtell

INTRODUCTION

The DOL has teamed up with the United States Postal Service (USPS) to provide a platform that can be used by State Workforce Agencies (SWAs) to leverage the capabilities of In Person Proofing (IPP) at participating USPS locations. Features include the ability to retrieve a list of participating post offices closest to a provided address, ability to send claimant information to USPS to begin the IPP process using an enrollment code, and the ability to retrieve the results of the IPP.

BASELINE PROCESS

There are three main actors when using the DOL USPS IPP platform:

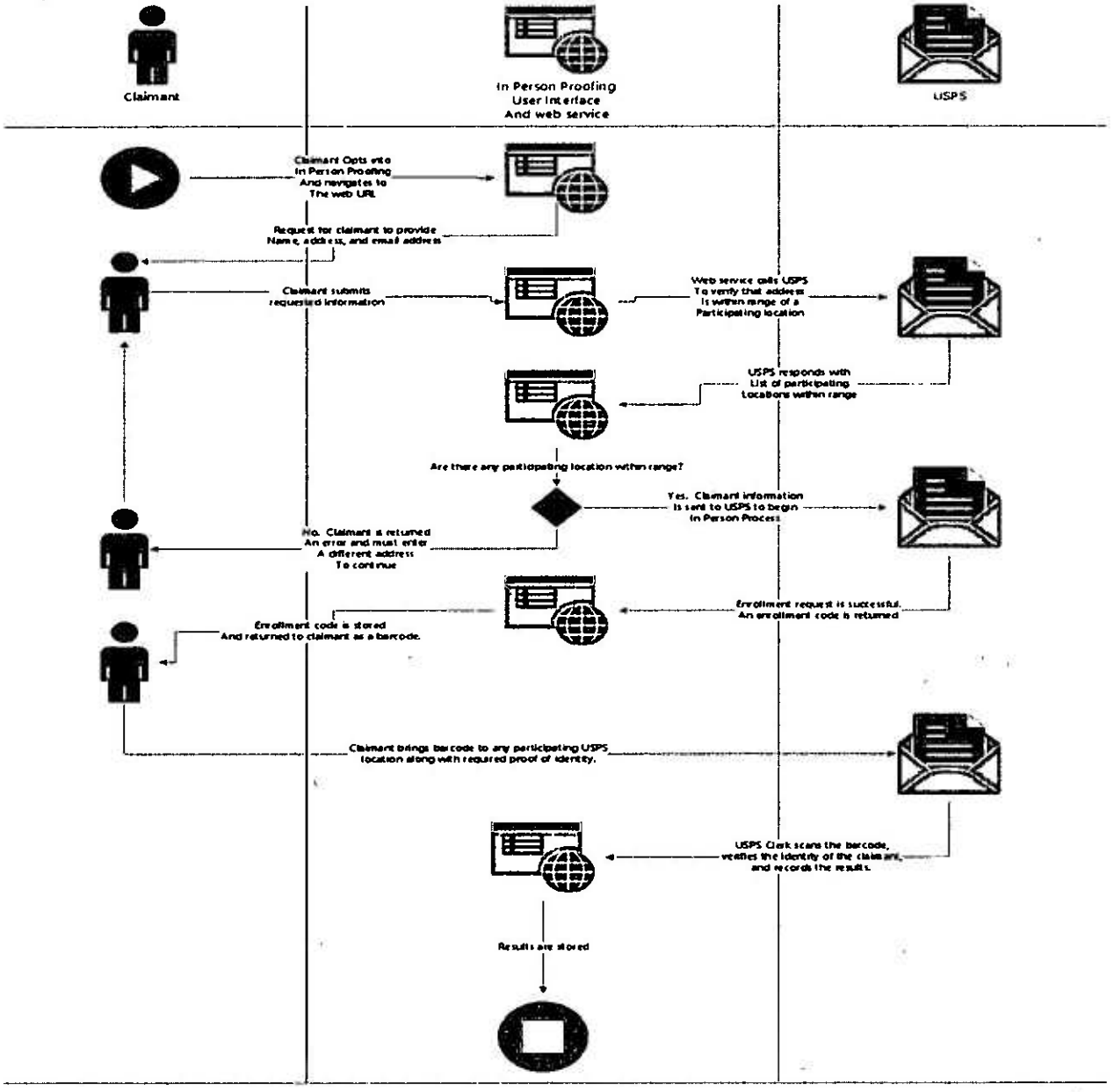
- Claimant – The applicant who is the subject of identity proofing.
- State Workforce Agency – The organization that needs the claimant to perform proofing. Also makes web service calls to the DOL Platform to retrieve the results.
- DOL Platform – The web service platform used as an intermediary between the State Workforce Agency, and USPS. If the DOL user interface is leveraged, then also used by the Claimant.

The typical IPP process occurs in three phases:

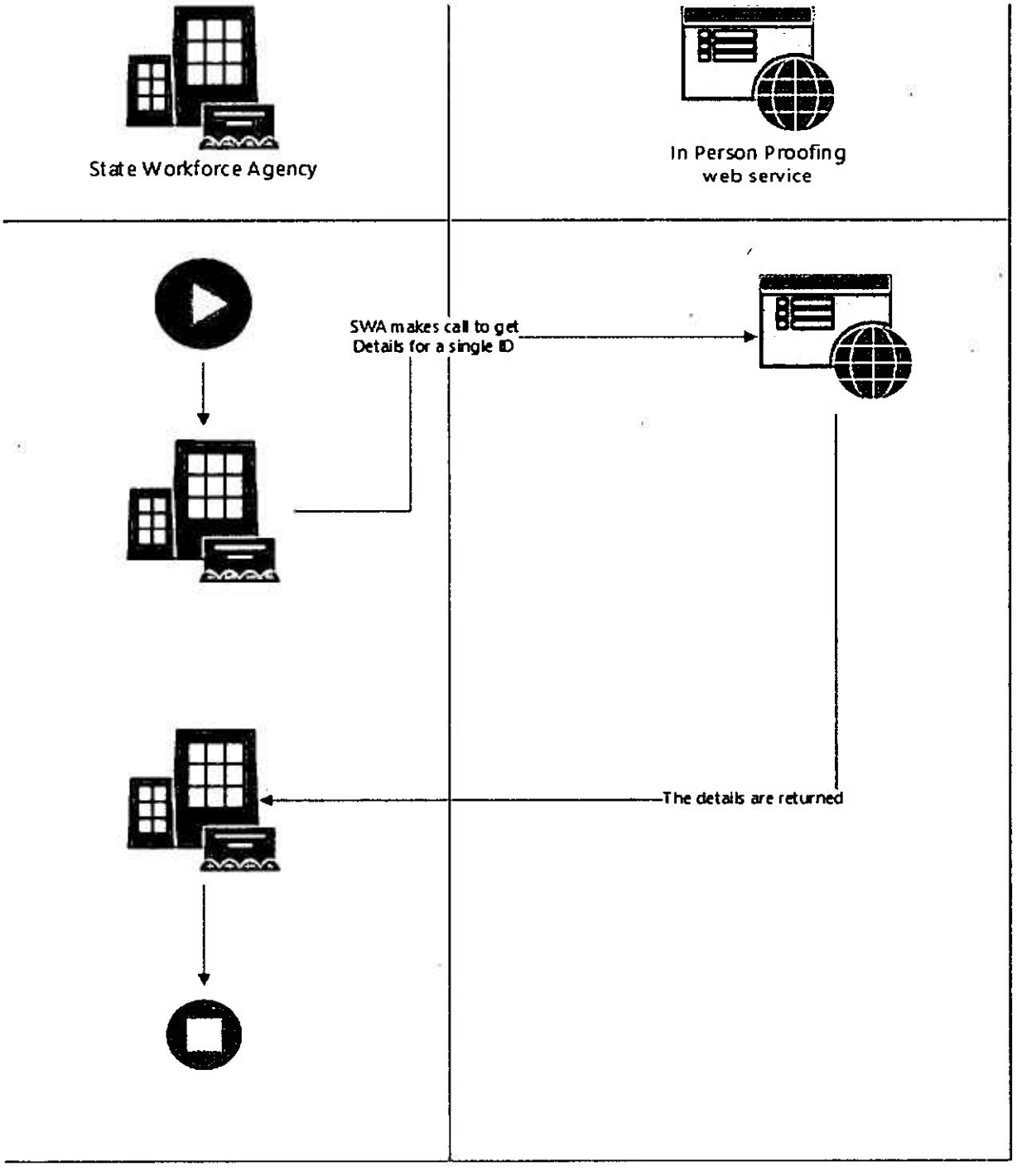
1. Initial Web Session. During this phase the State Workforce Agency or, if using the DOL UI, claimant, interact with the DOL platform to verify that there are one or more participating USPS locations within 50 miles and to initiate the enrollment process with USPS. A temporary enrollment code is returned. The enrollment code will be presented as both a barcode and a number that is used to link the claimant between phase 1 and phase 2.

2. In-Person Session. During this phase the claimant presents the enrollment code, in the form of a barcode or number, along with their identification documents. A combination of equipment, software, and USPS staff will be used to perform the proofing.
3. Return Web Session. After the user has completed IPP, the results will become available on the DOL platform. State Workforce Agencies can leverage provided result endpoints to retrieve information related to the status of the IPP session(s). Desired future state includes ability to provide the DOL platform with a webhook so that the DOL platform can initiate sending results to State Workforce Agencies instead of State Workforce Agencies needing to poll for changes.

CLAIMANT FLOW



STATE WORKFORCE AGENCY RESULTS FLOW



WEB APPLICATION URL

These URLs are used with the DOL frontend.

WITH CHOICE SCREEN:

Stage:https://stage1-unemployment.dol.gov/start/XX/?swa=XX&swa_xid=XXXXXXXX-XXXXXX-XXXXXXX-XXXXXXXXX&lang_cd=en
Production: https://unemployment.dol.gov/start/XX/?swa=XX&swa_xid=XXXXXXXX-XXXXXX-XXXXXXX-XXXXXXXXX&lang_cd=en

DIRECTLY TO THE USPS OPTION:

Stage: https://stage-arpaui-ipp.dol.gov/search?swa_xid=XXXXXXXX-XXXXXX-XXXXXXXX-XXXXX&swa=XX&lang_cd=en
Production: https://arpaui-ipp.dol.gov/search?swa_xid=XXXXXXXX-XXXXXX-XXXXXXXX-XXXXX&swa=XX&lang_cd=en

WEB SERVICE APIS

The DOL Platform utilizes the Representational State Transfer (REST) web service architecture. REST is a lightweight alternative to other web service mechanisms such as SOAP and WSDL. It relies on stateless, client-server, cacheable communications protocol. HTTPS protocol is required.
The DOL Platform URLs are environment specific. The production environment is available to all IP addresses with a geolocation in the US. Lower environments are only available to whitelisted IP addresses. The expectation is that State Workforce Agencies will be able to use the pre-production, stage, environment for their testing. Lower environments (dev and test) are generally reserved for the DOL development team's development and testing.

Dev: https://dev-arpaui-ipp.dol.gov/api/
Test:https://test-arpaui-ipp.dol.gov/api/
Stage: https://stage-arpaui-ipp.dol.gov/api/
Production: https://arpaui-ipp.dol.gov/api/

RESULT

Retrieve records associated with a provided swa_xid. Optionally provide an enrollment code to guarantee result is limited to a single record.

Endpoint URL	https://hostname/api/swa/[SWA_XID]
Request Type	GET
Request Parameters	enrollment_code – Optional. The value of the "enrollmentCode" key from the opt-in applicant call.
Request Headers	JWT
Success Response Body	{ "swa_xid": "20230418-141053-1134517-111000000", "records": [{ "enrollment_code": "2390001535117108", "first_name": "Test",

	"last_name": "McTest", "street_address": "135 Hickory rd", "city": "Clinton", "state": "AR", "zip_code": "72301", "email_address": "test@test.test", "expiration_date": "2023-04-25", "status": "In-person passed", "proofing_post_office": "CONGRESS HEIGHTS", "proofing_city": "WASHINGTON", "proofing_state": "DC", "primary_id_type_id": "State non-driver's identification card", "transaction_start_date_time": "11/15/2022 120313", "transaction_end_date_time": "11/15/2022 120313", "fraud_suspected": "False", "proofing_confirmation_number": "KVMSITDOLB20013", "time_created": "2023-04-18 20:00:29.367521+00:00", "time_updated": "2023-04-18 20:00:29.367528+00:00", "time_email_sent": "2023-04-18 19:10:19.120792+00:00" }] }
Additional Information	Requires authentication

Unset fields are omitted from the response.

Response fields:

Field	Description	Type/Format
swa_xid	The unique identifier shared between the state and DOL	Up to 255 Character String. Must be valid to use as a query parameter and not contain forward slash "/" or back slash "\"
error_message	If an error occurred, a description of the error	String
records	Contains the list of enrollment codes and supporting information associated with the swa_xid	Array
enrollment_code	The code used at USPS	Numeric String
first_name	The claimant's first name.	String

last_name	The claimant's last name.	String
street_address	The claimant's street address.	String
city	The claimant's city.	String
state	The claimaint's state.	2 letter abbreviation
zip_code	The claimant's zip code	String
email_address	The claimant's email address	String
expiration_date	A DOL configured number of days after the enrollment has started. Note: this isn't used since USPS doesn't accept a configurable expiration.	Date
status	Passed: The claimant completed the proofing transaction successfully.	"In-person passed",
	Failed: The claimant completed the proofing transaction unsuccessfully.	"In-person failed",
	Expired: The enrollment code has expired	"In-person expired",
	Absented: The enrollment has not expired, and the claimant has not completed enrollment.	"In-person absented",
	Not-exist: USPS indicates that the enrollment code does not exist.	"In-person not-exist"
failure_reason	A description of why the customer failed in-person proofing.	String
proofing_post_office	The name of the post office that performed the transaction.	String
proofing_city	The city of the post office that performed the transaction.	String
proofing_state	The state of the post office that performed the transaction.	2 letter abbreviation
primary_id_type	A description of the ID that was presented during the transaction.	String
secondary_id_type	If present, a description of the secondary ID that was presented during the transaction.	String
transaction_start_date_time	The date and time that the in-person proofing transaction started. Note: this is a pass-through from USPS and appears to have a bug in the time.	Date and time*
transaction_end_date_time	The date and time that the in-person proofing transaction ended. Note: this is a pass-through from USPS and appears to have a bug in the time.	Date and time*
fraud_suspected	An indication of whether fraud was suspected by the Postal Clerk	"True" or "False"
proofing_confirmation_number	A confirmation number for the in-person proofing event. Generated by USPS.	String
response_message	Response message from USPS indicating the results of the call to get proofing results.	String
time_created	When the record was recorded in the DOL system.	Date and time with timezone

time_updated	When the record was last updated in the DOL system.	Date and time with timezone
time_email_sent	Date and time DOL sent an email to the claimant. Only applies to states using DOL frontend.	Date and time with timezone
time_email_reminder_sent	Date and time DOL sent an email reminder to the claimant. Only applies to states using DOL frontend.	Date and time with timezone

Attachment 6 – API call requirements for login.gov results.

LOGIN.GOV ONLINE PROOFING: ENDPOINT DEFINITION AND USAGE

Version 0.1
06/05/2023

DOCUMENT IDENTIFICATION INFORMATION	
Version:	0.1
Date Created:	06/05/2023
Created By:	Xavier Wofford
Date Published:	DRAFT

Change History			
Version	**Date**	**Description**	**Author**
0.1	6/05/2023	Add endpoint descriptions	Xavier Wofford

INTRODUCTION

The DOL has teamed up with the Login.gov Online Identity Verification Service to provide a platform that can be used by State Workforce Agencies (SWAs) to leverage the capabilities of online identity verification. Features include the ability to retrieve the results of the identity verification, update the status of the results, or remove the results from the DOL platform.

BASELINE PROCESS

There are three main actors when using the DOL USPS IPP platform:

- Claimant – The applicant who is the subject of identity proofing.
- State Workforce Agency – The organization that needs the claimant to perform proofing. Also makes web service calls to the DOL Platform to retrieve the results.
- DOL Platform – The web service platform used as an intermediary between the State Workforce Agency, and Login.gov. The DOL user interface is also used by the Claimant to access Login.gov.

The typical Login.gov process occurs in three phases:

1. Web Session. During this phase the claimant interacts with the DOL platform to generate a unique authorization link that redirects them to Login.gov. The claimant then verifies their identity at IAL1 on the Login.gov site.
2. Intermediate Web Session. After the claimant has completed IAL1 verification with Login.gov, they are briefly sent to the DOL platform with a unique code that is used by the DOL to retrieve the claimant's information from Login.gov. Once their information is retrieved, the claimant is returned to Login.gov to ID proof.
3. Return Web Session. After the user has ID proofed with Login.gov, they are once again returned to the DOL platform with a unique code that is used to retrieve additional claimant information from Login.gov. State Workforce Agencies can leverage the provided swa endpoint to retrieve claimant verification information, update the status of the claimant verification information, or remove the claimant verification information from the DOL platform.

WEB SERVICE APIS

The DOL Platform utilizes the Representational State Transfer (REST) web service architecture. REST is a lightweight alternative to other web service mechanisms such as SOAP and WSDL. It relies on stateless, client-server, cacheable communications protocol. HTTPS protocol is required.

The DOL Platform URLs are environment specific. The production environment is available to all IP addresses with a geolocation in the US. Lower environments are only available to whitelisted IP addresses. The expectation is that State Workforce Agencies will be able to use the pre-production, stage, environment for their testing. Lower environments (dev and test) are generally reserved for the DOL development team's development and testing.

Dev: https://dev1-unemployment.dol.gov/
Test: https://test1-unemployment.dol.gov/
Stage: https://stage1-unemployment.dol.gov/
Production: https://unemployment.dol.gov/

SWA – GET ALL CLAIMS

Get all the encrypted claims in the queue that have not yet been marked as fetched.

Endpoint URL	https://*hostname*/swa/v1/claims/
Request Type	GET
Request	To access the additional pages of encrypted claims in the queue, add the parameter *?page=[page number]* to the URL. This will also be indicated by the "next" key in a successful response.
Request Headers	JWT

Success Response	{
	"total_claims": 188,
	"next": "https://unemployment.dol.gov/swa/claims/?page=2",
	"claims": [
	{
	"claim": {
	"ciphertext": "EpZJmAzjk4SQSQoPm0cSa9SH7NxfeygIp_1I1BUaMUUc1fEGzha
	K-6O8zWabYz16kgeGF3kUcGyh8sUdh4E1zM8BeQuUHbzgEA4U8NgRpm-
	0HHu1cVSln0p6w0ypMjI86e_0cciJV8hfnFiwrku_C0zbvcQ2KbF68EqjlxppV_NG06AnAU
	mJnZKUxEItvARVL8OJQ_72m2VVHvYrURU3eukhXkW4mycrejw-
	VRsSyikfyk8BYBJkL_xs6moZOdl8Zte9KcEI95T_8_EgHNdzpQgAzWqK-
	f9L8qdKt6ewibAnPjmxzRe470ih_MZUN42m-
	JSZzOYNKtru5GJaJmAFzGYU1qkDojS2otXy5S3a1tSWLkLf2K5jKQyQs70Y_usFKplceTy62c
	iZG-
	6U2lojhz_dg8hEXwfoN2WvcJky5sI6yX_0dtPwbxU99vE8ZxhwfwTQgMSd6ApDW5uvUh
	Wzge8YcgZAhLLhI3feBECOnX2XvHQEESg29w1OIYK4CYEXLUyZk7-a7_Hhs-
	WPzG1WwXgeylwV1QV4l61qxfkfc8wcsL1-c6c5E6UcpCY",
	"encrypted_key": "UGB3jWgHMqq7qjJSVr0iRLU7fUuzHZ1Vn42YimPGmE7A9s
	1_CPyL0g",
	"header": {
	"epk": {

	"crv": "P-256", "kty": "EC", "x": "8SN-7BlhNi7jeR1NmzoPUihxY7sCHevWFVLoEjZqMfA", "y": "Yf7TKi6H1OCtwVU6ZoyBvCPnWWLb89eiOg13f-csAZ8" } }, "iv": "QrU2cNhJtfRvFB0J", "protected": "eyJhbGciOiJFQ0RILUVTK0EyNTZLVyIsImVuYyI6IkEyNTZHQ00iLCJraWQiOiJrSmpqbXI0bEZ2RGZQZ19seEpJN19aaHBBMHlDdm5FZ2tJYk1ZVjhWNGpJIiwidHlwIjoiSldFIn0", "tag": "Vbh91J0RJOHBtNwMF6TvxA" }, "claim_id": "338c73f2-ae56-4c05-8eb1-bac3fe39deb8", "public_kid": "kJjjmr4lFvDfPg_lxJI7_ZhpA0yCvnEgkIbMYV8V4jI" }, ... }
Additional Information	Each claim is encrypted using the public key provided by the SWA and can be decrypted using the SWA's private key.

Decrypted Ciphertext Response fields:

Field	Type / Value	Description	Availability
id	String	The unique identifier for the claimant's claim in the DOL system	IAL1/ID-proofed
swa_xid	String	The unique identifier shared between the state and DOL	IAL1/ID-proofed
claimant_id	String	A unique identifier for the claimant in the DOL system	IAL1/ID-proofed
identity_provider	String	The entity that provided the identity verification results	IAL1/ID-proofed
identity_assurance_level	Int	1: The claimant completed identity verification at IAL1 2: The claimant completed ID-proofing	IAL1/ID-proofed
first_name	String	The claimant's first name.	ID-Proofed
last_name	String	The claimant's last name.	ID-Proofed
ssn	String	The claimant's social security number.	ID-Proofed
birthdate	String	The claimant's date of birth.	ID-Proofed
address	String	The claimant's street address.	ID-Proofed
city	String	The claimant's city.	ID-Proofed
state	2 letter abbreviation	The claimant's state.	ID-Proofed
zip_code	String	The claimant's zip code	ID-Proofed
phone	String	The claimant's phone number	ID-Proofed

email	String	The claimant's primary email address	IAL1/ID-proofed
all_emails	Array	A list of all email addresses associated with the claimant's account.	IAL1/ID-proofed
validated_at	Datetime	When the claimant's Login.gov payload was last validated by the DOL system.	IAL1/ID-proofed
verified_at	Datetime	When the claimant's identity was last verified by Login.gov	IAL1/ID-proofed

SWA – GET CLAIM WITH SWA_XID OR UUID

Get details on a specific claim using its swa_xid or its universally unique identifier (UUID).

Endpoint URL	https://*hostname*/swa/v1/claims/[swa_xid or UUID]
Request Type	GET
Request	N/A, no body or parameters are used.
Request Headers	JWT
Success Response	{ "id": "5837b135-95c8-4e05-a6e2-ca0031426aaa", "swa_xid": "20230614-141053-1134517-000040404", "created_at": "2023-06-14 17:42:51.498963+00:00", "updated_at": "2023-06-14 17:44:31.131319+00:00", "claimant_id": "cd7a91d831dbcddefd3b6184a64c9eee47f34858075f4f4e47af44e1e3b43f86", "events": [{ "happened_at": "2023-06-14 17:42:51.573302+00:00", "category": "Submitted", "description": "" }, { "happened_at": "2023-06-14 17:42:53.650825+00:00", "category": "Stored", "description": "eta-dev-arpa-ui-claims" }, { "happened_at": "2023-06-14 17:44:30.637718+00:00", "category": "Initiated With Swa Xid", "description": "" }, { "happened_at": "2023-06-14 17:44:30.752574+00:00", "category": "Submitted",

```
        "description": ""
      },
      {
        "happened_at": "2023-06-14 17:44:30.772473+00:00",
        "category": "Completed",
        "description": ""
      },
      {
        "happened_at": "2023-06-14 17:44:31.128003+00:00",
        "category": "Stored",
        "description": "eta-dev-arpa-ui-claims"
      },
      {
        "happened_at": "2023-06-14 19:10:53+00:00",
        "category": "Initiated With Swa Xid",
        "description": "2023-06-14T19:10:53+00:00"
      }
    ],
    "status": null
}
```


SWA – UPDATE CLAIM STATUS

Update the status of a specific claim.

Endpoint URL	https://*hostname*/swa/v1/claims/[swa_xid or UUID]
Request Type	PATCH
Request	{"status": "*new status*"}
Request Headers	JWT
Success Response	{"status": "ok"}

SWA – MARK CLAIM AS FETCHED

Mark a specific claim as Fetched so that it is removed from the claim queue.

Endpoint URL	https://*hostname*/swa/v1/claims/[swa_xid or UUID]
Request Type	PATCH
Request	{"fetched": "true"}
Request Headers	JWT
Success Response	{"status": "ok"}
Additional Information	Marking a claim as fetched will remove it from the encrypted claim queue for future Get All Claims requests.

SWA – MARK CLAIM AS RESOLVED

Mark a specific claim as Resolved.

Endpoint URL	https://*hostname*/swa/v1/claims/[swa_xid or UUID]
Request Type	PATCH
Request	{"resolved": "*reason for resolution*"}
Request Headers	JWT
Success Response	{"status": "ok"}

Exhibit #2

US Department of Labor

PII Breach Notification Plan

Document Number PII BNP 23

REDACTED

This Document has been redacted to protect sensitive IT Security information.