INTEGRITY

NASWA UI Integrity Center

In Partnership with USDOL

Request for Proposal

Centralized Identity Verification Service

October 23, 2019

Contents

Introduction

The Unemployment Insurance (UI) Integrity Center (Center) was established to develop "innovative UI program integrity strategies to reduce improper payments, prevent and detect fraud, and recover any improper payments made." [http://wdr.doleta.gov/directives/attach/UIPL/UIPL_28_12_Acc.pdf] The efforts of the Center are managed by the National Association of State Workforce Agencies (NASWA), Center for Employment Education and Research (CESER) under a cooperative agreement with the US Department of Labor (USDOL).

One of the Center's current tasks is to define, develop, test, and implement a centralized identity verification/identity proofing service to State Workforce Agencies (SWA's). This **Identity Verification Service (IDV)** will operate as a part of the Center's Integrity Data Hub (IDH) and the output of the IDV service will be provided to the SWA's along with other cross-matching and analysis from the IDH.

Purpose of This RFP

In September 2019, the Center received funding from USDOL to provide a **centralized** IDV service to address the need for SWA's to incorporate identity verification into their UI claims process, leveraging the existing IDH infrastructure and processes. As such, the Center is seeking industry partner(s) to provide the Center with a software-as-a-service (SaaS) Identity Verification/Identity Proofing capability.

The Center is seeking a solution that will deliver a determination of identity validity based upon information presented to the vendor through the IDH. For this purpose, the Center is requesting responses from qualified vendors capable of utilizing their products and services with the IDH to validate a UI claimant's self-attested information.

Reponses must be received electronically by 5:00 p.m. Eastern Standard Time on December 6, 2019 at DataHubRFP@naswa.org.

Questions regarding this RFP and additional information on the Data Hub technical architecture should be submitted to DataHubRFP@naswa.org.

Background

Since 2010, the UI Program has had an Improper Payment Rate (IPPR) of 10 percent or more. From July 2017 to June 2018, the most recent year for which data is available, the national improper payment rate as determined by the UI Programs' Benefit Accuracy Measurement (BAM) was estimated at 13.05 percent. [https://www.dol.gov/sites/dolgov/files/OPA/reports/2018annualreport.pdf] This represents an estimated $3.7 billion in improper payments nationally.

Identity fraud issues contribute to the improper payment rate, but due to a lack of consistent detection, data collection, date reporting, and administrative actions, the amount of identity fraud is currently difficult to accurately quantify.

Identity theft is a growing concern nationwide. According to the Department of Justice, Bureau of Justice Statistics, 17.6 million Americans experienced identity theft in 2014, and two-thirds of these

individuals experienced a financial loss because of the identity theft.[1] In 2015, the DOL Office of Inspector General (DOL-OIG) issued an Investigative Advisory Report that noted specific multiple-claimant identity theft schemes had proliferated in states over the previous years.[2] In the 2018 DOL Agency Financial Report, the DOL-OIG again noted that, "… fraud continues to be a significant threat to the integrity of the Unemployment Insurance (UI) program, as identity thieves and organized criminal groups have found ways to exploit program weaknesses."[3] As fraud threats continue to evolve with sophisticated schemes and attacks, the U.S. Department of Labor (DOL), Employment and Training Administration (ETA) must work to protect the sensitive information entrusted to the federal-state UI program and ensure that benefits paid from the UI trust fund are paid only to its intended beneficiaries.

SWAs currently cross-match UI claims against a variety of data sources in order to verify the eligibility of individuals for benefits. These data sources include certain Federal and state sources of incarceration and mortality records, fraud analytics tools, and – in limited instances – some form of identity verification. However, the implementation of these tools is inconsistent across the UI system.

While unemployment is currently at an historical low, the threat of fraud continues, and is increasing.

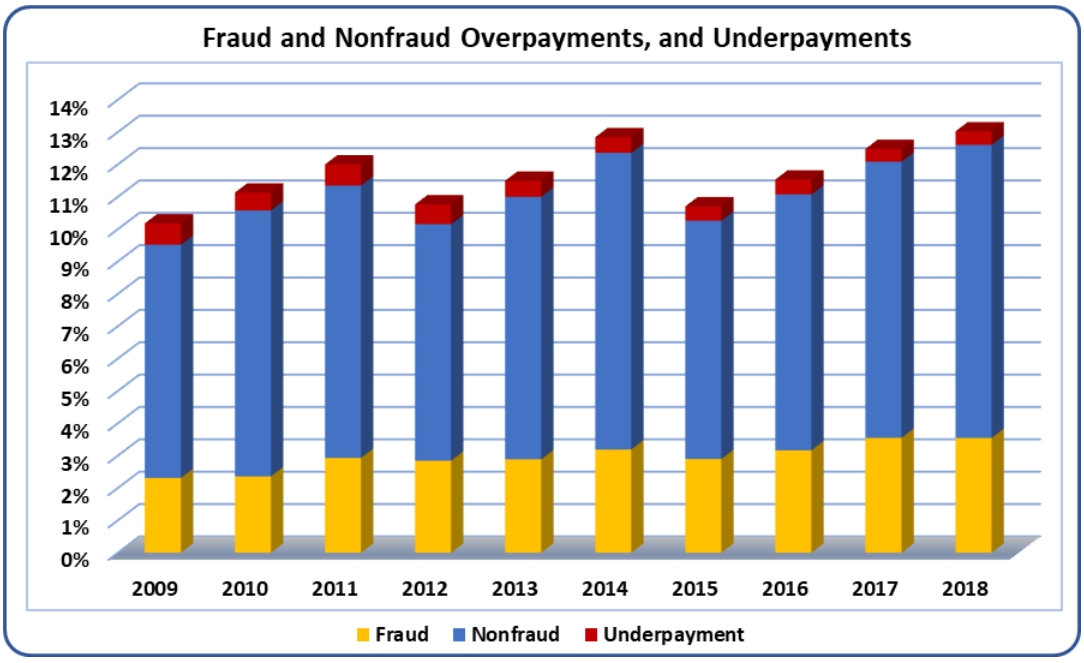


Figure 1: Improper Payments

Identity fraud in UI claims occurs in a few primary categories:

- Account take over: the attacker obtains control of a previously authenticated user's credential set, typically a result of a social engineering, phishing, brute force attack, or unintentional exposure;

[1] http://www.bjs.gov/index.cfm?ty=pbdetail&iid=5410
[2] https://www.oig.dol.gov/public/reports/oa/viewpdf.php?r=50-15-001-03-315&y=2015
[3] https://www.dol.gov/sites/dolgov/files/OPA/reports/2018annualreport.pdf

- Synthetic/Fake identities: the attacker utilizes identities that are fabricated, potentially with some accurate information, that are then made to appear as valid identities via credit bureau activity to enable the application for benefits; and
- Stolen identities: the identities of identity theft victims are utilized for an application for benefits.

In all cases, the analysis of active UI claims indicates there exists an ever-increasing presence of fraud, and an increase in fraud perpetrated by organized entities creating sophisticated attacks that have increasing scope.

All these types of identity fraud can be used in stand-alone attacks, or as a part of a larger fictitious employer attack. The breadth of the attacks creates a need for cross-state, cross-agency, and cross-industry data sharing/matching to detect and address the growing identity fraud problem.

The IDV Project has the goal of reducing the incidence of improper payments due to identity fraud while collecting data to establish additional steps to be implemented to continue to address the ever-changing Identity fraud problem.

Integrity Data Hub

The IDH is a secure, centralized multi-state data analysis tool which allows participating SWAs to submit claims for analysis and cross-matching against multiple data sources. Participating SWA's can select between various manual and automated communications channels based on the varying levels of resources and technology available to their UI agency. Communication channels include manual processes such as one-off lookups using the Data Hub website or spreadsheet upload. More automated channels such as secure FTP and web services are available. Currently the IDH cross-matches the submissions against the list of suspicious email domains and SWA submitted data within the Suspicious Actor Repository (SAR).

The IDH project team has developed a multi-component, phased plan to enhance the IDH. This plan is summarized in Figure 2, below. For **Phase 2** of the IDH, the Center is expanding the capabilities of the IDH to include: interfacing with additional data sources for expanded cross-matching, establishing a multi-state database of UI claims, providing an IDV service (the target of this RFP) and providing data analysis and reporting.

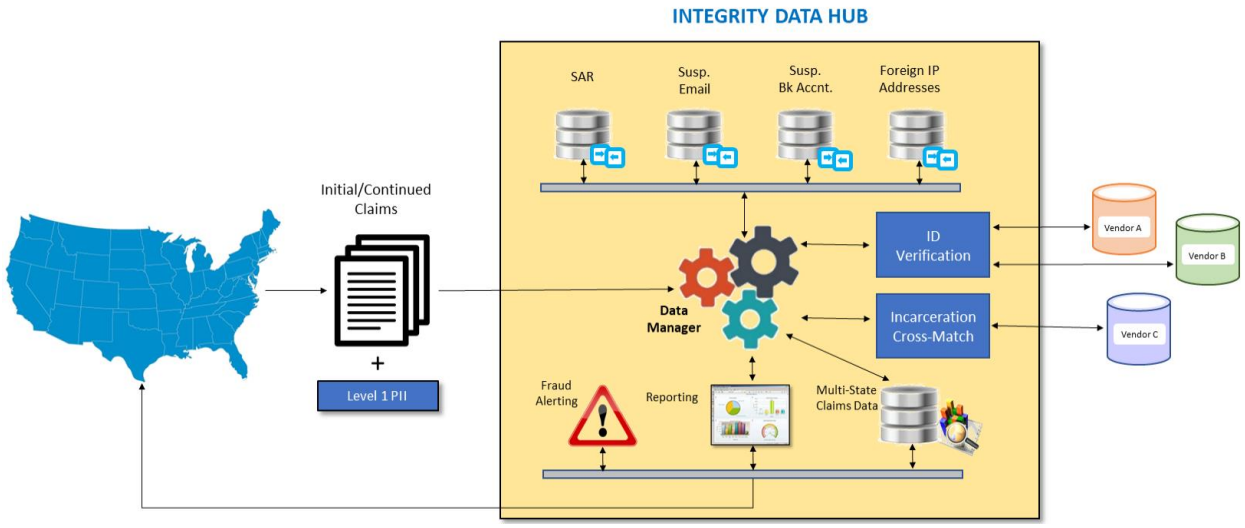


Figure 2: Data Hub Phase 2 Concept

IDV Functionality Objective

The Center is currently working with participating SWA's to collect regular/ongoing submission of all initial and weekly UI claims data. The IDH will serve as a centralized data repository and transmit each SWA's data to the IDV vendor at regular intervals including real time and routine batch processes. The IDH project team and vendor will develop and implement the integration and formatting of the exchanged data as part of the statement of work.

The IDV vendor will execute identity verification against this claims data and provide the results back to the IDH including a set of Identity verification indicators. Upon completion of the verification analysis, all claims data transmitted to the IDV vendor will be permanently and verifiably deleted and not stored by the vendor in any fashion.

The IDV solution is expected to function in a solely passive fashion, without a need for direct claimant interaction with the IDV vendor. No "out of pocket" or "out of wallet" information will be requested of the claimant.

Responding vendors may use dataset (s) available through financial institutions such as credit reporting agencies and additional public, private, and proprietary data sources designed to prevent and detect potential identity and/or UI improper payment fraud. These datasets will provide SWAs access to: (1) real-time claimant identity verification and identity risk assessments, and (2) risk attributes associated with the identity analysis.

The Center's IDV service is expected to function as an augmentation of the current IDH, and minimally impact the SWA-specific processes for handling electronic UI claims already in place. This augmentation is currently envisioned as an additional set of indicators returned in an expanded IDH SAR Matching Report for each submitted claim. The current matching report format is shown in Appendix A.

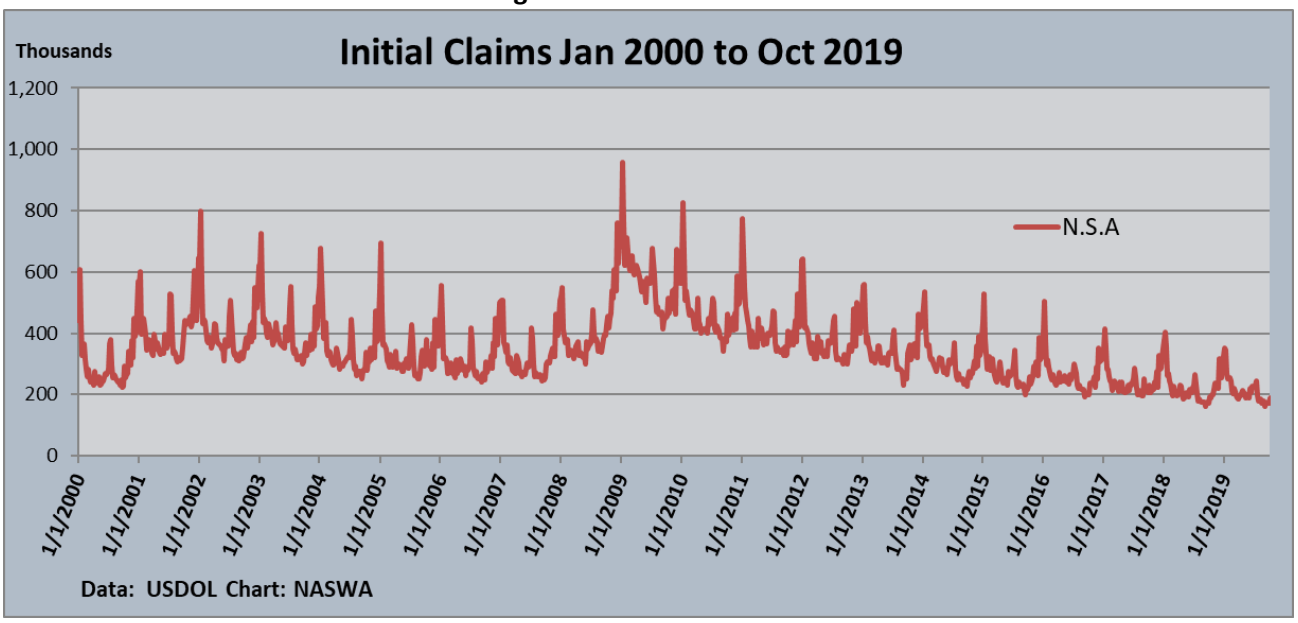
An overview of the proposed Identity Verification Service architecture is shown in Appendix A.

The Identity Verification Service architecture utilizes an open source software stack in an AWS cloud-based environment according to NIST based best practices. The open source stack currently includes Red Hat Linux, Apache Httpd, Apache Tomcat, and Apache Cassandra. OpenAM and OpenDJ are used for single sign on. The AWS cloud-based environment provides scalability, flexibility, availability and can be managed with a small team. The architecture includes a web tier, application tier, and database tier while currently supporting the SSO login application and additional Center applications. Interfaces to SWA IT systems is accomplished in Phase 1 via bulk FTP uploads and API transactions of claim data – including the PII information required to perform the Identity Verification Service tasks. The data will be presented to the selected vendor(s) for verification/proofing/validation with the scoring and response returning to the IDH and subsequently be delivered to the SWA within the augmented reporting capability.

Transaction Volume

The volume of Identity Verification requests is dependent on the number of Initial UI claims filed and adoption by the SWA's and will increase as SWA participation increases. Current volume (based on the number of states participating) is anticipated to be approximately 40,000 verification requests per week, with a volume of up to approximately 300,000 verification requests per week – when all SWAs are participating and with the current unemployment rate. The unemployment rate is cyclical, and the volume of UI Initial Claims will follow the overall trend as displayed in Figure 3, below.

Figure 3: Initial Claims



Anticipated Solution

The selected vendor solution is expected to meet the following criteria:

1. Passive claimant Identity Verification/Proofing/Validation shall be delivered from the data elements defined below. Passive is defined as verification completed from data transmitted by the IDH to the IDV vendor for verification, with no additional interaction with the claimants i.e. no "out of pocket" or "out of wallet" information will be requested of the claimant.

   The claims data elements transmitted to the IDH and available to the IDV solutions includes the following:

   - First Name
   - Middle Initial
   - Last Name
   - Social Security Number (SSN)
   - Date of Birth (DOB)
   - Email address
   - Address(s) (as reported by claimant)
   - Phone Number(s)
   - IP Address
   - Financial Institution Routing Number for Benefits Distribution
   - Financial Institution Account Number for Benefits Distribution

2. Process both individual requests via API and bulk requests of multiple identities via batch processing.

3. Information used to evaluate the identity should be matched through multiple sources of data to increase the accuracy of the evaluation and decrease the likelihood of false positives. Examples of data sources may include, but not be limited to:

   a. Consumer Credit Information and/or other financial data;
   b. Social Security Administration information;
   c. Known address information;
   d. Telecommunications Information; and
   e. Billable utilities information.

4. The processes utilized to determine identity scoring should include pattern matching and recognition and evaluation of the information provided to determine identity risk. Process should include (but not be limited to):

   a. Fraudulent behavior checks based on (vendor specific) fraud indicators;
   b. Pattern recognition (i.e. multiple verification checks, multiple address checks, etc.);
   c. Address checks (valid, deliverable, associated with individual, etc.);
   d. The processes should return a risk score as determined by the vendor, this score shall indicate the risk associated with the information presented. At a minimum the solution should indicate:
      i. Synthetic/Fake Identity;
      ii. Known Compromised (stolen) Identity;
      iii. Ranking of Fraud Potential;

iv. Ranking of Other Issues; and
v. In conjunction with the score cause codes related to the score should be provided.

5. The solution should have the widest reach possible. A target for the IDV solution is to have information returned for 95 percent of the claims submitted for verification. **Vendors should specify in their proposal a match rate that maximizes the number of returns to the IDH.** Included in this population will be individuals who:

    e. Are unbanked, or underbanked;
    f. Lack traditional residency history; and
    g. Lack traditional employment history.

Solution Requirements

The selected vendor solution will meet the following requirements:

1. Adhere to the requirements outlined in Restrictions Against Disclosure including;
    a. Privacy Breach Notification Requirements;
    b. System and Data Security; and
    c. Background Investigation Requirements for operational and implementation resources.
2. Provide a project implementation plan describing the IDV data service deliverables and establish the schedule for the IDV's implementation of IDV data services.
3. In conjunction with the IDH project team, develop a Statement of Work (SOW) covering timelines, data interaction specifications, and transaction performance metrics.
4. Conduct testing of the IDV solution, in coordination with the IDH project team, to include functional and load testing to ensure the IDV vendor meets the business and technical requirements included in this RFP and co-developed in the SOW.
5. Have in place a cyber-insurance policy that provides coverage for network security, privacy risks, and data security breaches, prior to pilot state implementation.
   Vendor shall participate in weekly meetings with IDH during implementation, and routine status meetings for the remainder of the period of performance to help ensure that the IDV solution implemented in coordination with the IDH meets the project plan and schedule, adheres to the business and technical requirements including industry standards for providing real-time and accurate IDV responses to the IDH.

Restrictions Against Disclosure

The Vendor implementation of the IDV solution will involve access to confidential data including UI Claimant Personally Identifiable Information (PII). All Vendor staff including subcontractors will be required to sign non-disclosure agreements.

The Vendor, in coordination with the IDH project team, will develop and implement the integration and formatting of the data exchange as part of their agreed upon statement of work. All UI Claimant PII provided by the Integrity Center IDH shall be permanently deleted by the Vendor in a verifiable fashion

upon completion of the IDV transaction. For details, refer to National Institute of Standards and Technology (NIST) Publication SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010.

System and Data Security

The Vendor shall integrate Cybersecurity Risk Management into IT system and service planning, delivery, and management to stay consistent with the NIST Cybersecurity Framework and the System Development Life Cycle (SDLC).

The Vendor is subject to all federal security law, rules, regulations, guidance and standards applicable to the product and/or service offered, pursuant to the following authorities (including but not limited to):

The confidentiality, integrity, and accessibility of information and information systems:

(a) Public Law 113-283, Federal Information Security Modernization Act (FISMA) of 2014
(b) OMB Circular No. A-130, Managing Information as a Strategic Resource

The use of common security configurations:

(c) Federal Acquisition Regulation (FAR), Part 39 of Federal Acquisition Regulation
(d) NIST Special Publication 800-70, National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

The IDV implementation, in accordance with the Federal Information Security Management Act (FISMA) and NIST Special Publication 800-60, shall be considered a security classification of "Moderate". Therefore, this system shall be required to follow the corresponding minimum-security controls, processes, and protocols defined in NIST Special Publication 800-53[4]. These controls include, but are not limited to:

1. Data Transmission and Storage:
   - Use of encryption for all data at rest and during transmission
     - All data is encrypted using asymmetric encryption with all transition methods/channels
   - Ensure claimant data provided by the Center for IDV purposes is purged from the system following processing
   - Claimant data from the Center is not shared with any other entity, and matching results from requests are only available to the Center
   - Ensure that all data stored using cloud-based infrastructure resides on servers based in the United States

2. System Access and Monitoring:
   - Access to the IDV system and associated data is restricted to authorized users
     - The Vendor shall comply with personal identity verification procedures for staff and include this requirement in all contracts/subcontracts when the contractor/subcontractor has access to Center data
     - Restrict access of Vendor staff to production system/data and limit access to Center data by contractors and/or subcontractors
     - Functionality available to Vendor's users will be based on user role

[4] https://nvd.nist.gov/800-53

- Bi-annual validation and re-certification of all system user accounts
- Ensure user access and all transactions are monitored
  - Maintenance of system logs to track user activity and transactions, including user ID and timestamp

3. Independent Security Assessments:
   - Conduct code-level static and dynamic vulnerability assessment and resolve software vulnerabilities at the application level prior to production implementation
   - Conduct penetration testing such as a simulated attack on the system to evaluate the security of the system prior to major system implementation or upgrade.
   - Conduct ongoing biennial penetration testing in conjunction with internal security assessments.

4. Adhere to Privacy Breach Notification Requirements:
   - Definitions
     - "Breach" is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where--
     - A person other than an authorized user accesses or potentially accesses PII; or
     - An authorized user accesses or potentially accesses PII for an unauthorized purpose.
     - "Information" is defined as any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic, or audiovisual forms (See Office of Management and Budget (OMB) Circular No. A-130, Managing Federal Information as a Strategic Resource).
     - "Information System" is defined as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).
     - "Personally Identifiable Information (PII)" is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular No. A-130, Managing Federal Information as a Strategic Resource).
   - Requirements:
     - Contractors and subcontractors who collect or maintain claimant information on behalf of the Center or uses or operates an information system on behalf of the Center, shall comply with Federal law e.g., FISMA 2014, E-Government Act and the Privacy Act. Additionally, the Vendor shall meet OMB directives and National Institute of Standards and Technology Standards to ensure processing of PII is adequately managed, including:

       a) Properly encrypt PII in accordance with appropriate laws, regulations, directives, standards or guidelines;
       b) Report to the Center any suspected or confirmed breach in any medium or form, including paper, oral, and electronic within one hour of discovery;
       c) Cooperate with and exchange information with IDH as well as allow for an inspection, investigation, forensic analysis, as determined necessary by the Center, in order to effectively report and manage a suspected or confirmed breach;

d) Maintain capabilities to determine what information was or could have been compromised and by whom, construct a timeline of user activity, determine methods and techniques used to access Center information, and identify the initial attack vector;
e) Ensure staff that have access to systems or information are regularly trained to identify and report a security incident;
f) Take steps to address security issues that have been identified, including steps to minimize further security risks to those individuals whose PII was lost, compromised, or potentially compromised; and
g) Report incidents in accordance with the Center's incident management policy and US-CERT notification guidelines.

- Remedy:
  a) A report of a breach shall not, by itself, be interpreted as evidence that the Vendor or its subcontractor (at any tier) failed to provide adequate safeguards for PII. If the Vendor is determined to be at fault for the breach, the Vendor may be financially liable for Center costs incurred in the course of breach response and mitigation efforts;
  b) The Vendor shall take steps to address security issues that have been identified, including steps to minimize further security risks to those individuals whose PII was lost, compromised, or potentially compromised; Additionally, the individual or individuals directly responsible for the data breach shall be removed from the contract within 45 days of the breach of data;
  c) The Center reserves the right to exercise all available contract remedies including, but not limited to, a stop-work order on a temporary or permanent basis in order to address a breach or upon discovery of a Vendor's failure to report a breach as required by this clause. If the Vendor is determined to be at fault for a breach, the Vendor shall provide credit monitoring and privacy protection services for one year to any individual whose private information was accessed or disclosed. The individual shall be given the option, but the decision is theirs. Those services will be provided solely at the expense of the Vendor and will not be reimbursed by the Center.

Background Checks

All contract/subcontract employees with access to PII data related to the IDV solution will require background investigation. The Vendor will certify to the Center that all staff including contract/subcontract employees have successfully completed the appropriate level of background investigation for each position used by the vendor on this project. The Vendor and its subcontractors (if any) will ensure that investigation requirements for employees are based on the risk or sensitivity level designation of the position. The Center informs the Contractor of the risk or sensitivity level for each contractor employee position. The minimum level of investigation for each risk or sensitivity level is:

Position Risk/Sensitivity Level:	Minimum Investigation Requirement:
Low Risk/Non-sensitive:	National Agency Check & Inquiries (NACI)

Moderate Risk:	Minimum Background Investigation (MBI)
High Risk:	Background Investigation (BI)
Noncritical-Sensitive:	Minimum Background Investigation (MBI)*
Critical-Sensitive:	Single Scope Background Investigation (SSBI)*

For positions with significant security responsibilities such as the ability change security controls, bypass and/or manipulate audit logs, and directly access and extract large amounts of data outside of normal user interfaces, the minimum risk designation shall be "High Risk". Occupations that frequently have significant security responsibilities include, but are not limited to, system administrators, database administrators, and developers.

Timeline

The RFP timeline of events:

RFP Activity	Timeline
Identity Verification RFP Webinar*	November 6, 2019
Final Clarification Questions	November 15, 2019
Questions and Responses Posted	November 22, 2019
Proposals Due	December 6, 2019
Offeror Presentations**	December 20, 2019
Best and Final Offer Pricing (optional)	January 10, 2020
Award (anticipated)	January 24, 2020

* The Webinar is designed to afford the opportunity for offerors to formulate additional questions and provide their input/comments. Webinar registration, a PDF copy of this RFP, and RFP questions and answers will be posted at http://www.itsc.org/Pages/IDV.aspx.

** Offeror presentations may be conducted with selected bidders determined to be within the competitive range for awards and may not include all bidders. Offeror presentations may be conducted virtually via web, or on-site at NASWA in Washington, DC. Travel and associated costs are the responsibility of the offeror.

The Center reserves the right to invite offerors to participate in detailed discussions, clarifications to responses, and presentations/demonstrations subsequent to the proposal due date.

Deliverable timeline:

Project Activity	Timeline
Conduct initial testing of IDV solution	March 20, 2020
Pilot solution available	April 15, 2020
Production solution available	September 18, 2020

Period of Performance

The Period of Performance for this procurement is 24 months from the date of the execution of the contract. If there is a delay in completion of the project, the parties may agree to extend the performance period as necessary, contingent on the availability of federal funds and provided there is no change in the scope of the work.

Proposal Submission Elements

The offeror's proposal submitted in response to this RFP shall include two parts - Part I – Technical and Part II – Business, as listed below. The proposal shall include a transmittal letter. The transmittal letter shall identify the solicitation name/number. The transmittal letter shall include the name and DUNS number of the firm submitting the proposal, the firm's address, and a contact name and phone number. The transmittal letter shall also identify any proposed subcontractors. The transmittal letter must contain a statement to the effect that the proposal is guaranteed for a period of at least one hundred and twenty (120) days from the date of proposal receipt by the Center.

Part I Technical		**FORMAT**	**PAGE LIMIT**
Factor A	Technical Approach	Written	20 pages total
Factor B	Staff Experience and Qualifications	Written	6 pages total
Factor C	Management Plan	Written	10 pages total

Part II Business		**FORMAT**	**PAGE LIMIT**
Factor D	Past Performance	Written	3 References, 6 pages total
Factor E	Cost/Price	Written	No Limit

Offerors must not exceed the page limits cited above. Proposals submitted in excess of the prescribed page limits shall be considered non-responsive and shall be removed from consideration.

Written parts of the proposal shall be formatted as follows:

Page Size:	8 ½ x 11" with at least 1" margins on all sides
Font Size:	12 point or larger
Page Numbering:	Pages consecutively numbered within each section
Page Count:	Title pages, tables of contents, and section dividers are not included in the page count
Format:	Two-column format is allowable

The Center takes seriously the intent of the Procurement Integrity and Ethics statutes. Any proposal found to be copied from a potential competitor is subject to disqualification and, therefore, ineligible for contract award. Price and Cost information must not be included in the Technical Proposal.

PART I – TECHNICAL

Factor A. TECHNICAL APPROACH

The offeror shall provide a detailed technical approach for performing and executing each of the tasks listed below for the IDV project in a manner that will provide the Center and IDH with cost effective and quality services.

1. Identity evaluation service:
   - Data transmission methods and associated file formats for interfacing with the IDH (API, ftp, etc.);
   - Rubric for evaluation data returned to the IDH. (with examples);
   - Additional flags/information returned for evaluation score, on a per identity basis (with examples);
   - Provide configuration capability for returned scores to be included in the expanded IDH SAR Report returned to the SWAs;
   - Provide accuracy rate for validation of **unique identities,** including false positive rate;
   - Provide appropriate utilization rate of the validated **unique identity** including false negative rate;
   - Provide IDV processing rate, including volume and concurrent request capacity rate; and
   - Provide detection of **synthetic/false identities** rate including the false positive.

2. Information security:
   - Provide verifiable deletion of all IDH provided data upon IDV completion; and
   - Provide data encryption for all IDH provided data, both at rest and in motion.

3. Data sources utilized for identity evaluation:
   - Provide offeror's authoritative data sources utilized;
   - Provide aging statistics for the data sources utilized;
   - Provide historical matching statistics for identities;
   - Provide historical false positive statistics for identifying potentially fraudulent activity;

- Provide description of similar services to other/past projects; and
- Provide the results/benefits provided on other/past projects.

4. Implementation and project management:
   - Provide examples of previous engagements implementing identity evaluation;
   - Provide description for preferred methods of the following for implementation:
     - Requirements gathering;
     - Solution integration with identity evaluation partner;
     - Testing and verification methodologies;
     - Estimating implementation timeline post requirements finalization; and
   - Ongoing communications with the UI Integrity Center project manager and project team.

Factor B: SYSTEM AND DATA SECURITY

The offeror shall provide copies of the two most recent information security compliance audits, including auditor information. Provide all Corrective Action Plans (CAP) and/or Risk Management Plans related to the two most recent information security audits. Provide all results of any CAP or Plan of Actions & Milestones (POAM).

Factor C: STAFF EXPERIENCE AND QUALIFICATIONS

The offeror shall provide three resumes (two pages maximum per resume) for key personnel to be assigned to the project for implementation of proposed solution. Resumes should include: name, proposed labor category, percentage of time allocated to the IDV project, and relevant work experience. The resume(s) shall include educational and training accomplishments, as well as past work and other relevant experience, including any special accomplishments and skills. Resumes shall include dates of employment, education, etc. Resumes may not exceed six total pages.

Factor D - PAST PERFORMANCE

The offeror shall provide three references, which include the Company/Agency name, address, contact, contact's phone number and the name of the project completed. The work shall be similar in scope (nature and size) to this RFP's statement of work. References must be in relation to work that was performed within the last five years.

Performance information will be used for both responsibility determinations and as an evaluation factor against which offerors' relative rankings will be compared to assure best value to the Center. The Center will focus on information that demonstrates quality of performance. References other than those identified by the offeror may be contacted by the Center. Names of individuals providing reference information about an offeror's past performance shall not be disclosed. References may not exceed six total pages.

Factor E: MANAGEMENT PLAN

A management plan shall include the following:

- A chart showing how the project will be organized, including all tasks and deliverables and the overall leadership, business management, task or team leaders, and staff for each part;
- A timeline or schedule of task and subtask starts, endings, and milestones; and
- A brief overview of how the project will be managed.

PART II - BUSINESS

Factor F – COST/PRICE

Offerors shall submit their quote with any and all transaction/unit costs, and any variation of transaction/unit cost presented as a function of volume must be clearly stated.

The offeror will provide cost estimates for the development, integration, and ongoing management of the project necessary to accomplish the tasks in this RFP. In addition, the offeror will provide proposed unit transaction costs based on the proposed solution and on the estimated initial claims workloads displayed in the table below.

The Center is interested in evaluating the cost/benefit of varying levels of service and data sources used for identity validation. As such, If the offerors solution includes varying/optional tiers of service, data sources, and/or identity verification services, such as the inclusion/exclusion or combination of data sets or proprietary processes, the offeror will clearly define and explain the pricing and functionality options that both include/ do not include these tiers.

Estimated Costs					IC's In % YR 1	Year One Vol	Cost/Trans Yr 1	IC's In % YR 2	Year Two Vol	Cost/Trans Yr 2
FY	Actual 2016	Actual 2017	Actual 2018	3 Yr Avg			TBD			TBD
Q1 Initial Claims	3,936,371	3,230,885	3,219,334	3,462,197	10%	346,220	$0	65%	2,250,428	$0
Q2 Initial Claims	3,273,476	2,925,529	2,698,555	2,965,853	20%	593,171	0	85%	2,520,975	0
Q3 Initial Claims	3,010,285	3,128,240	2,452,447	2,863,657	30%	859,097	0	90%	2,577,292	0
Q4 Initial Claims	3,873,459	3,426,888	3,985,603	3,761,983	46%	1,725,079	0	95%	3,573,884	0
Total Initial Claims	**14,093,591**	**12,711,542**	**12,355,939**	**13,053,691**		**3,523,567**	**$0**		**10,922,579**	**$0**

Note: The RFP does not commit the Center to pay any costs incurred in the submission of offer's quote or to contract for the services.

Evaluation Criteria

The NASWA project team will evaluate all proposals using the following evaluation criteria and award base contracts to the contractor(s) that represents the best value for NASWA.

The factors are presented in the order of importance (i.e., Factor A has the greatest weight, Factor B the second greatest weight, etc.). Non-price factors, when combined, are significantly more important than price.

Please be advised that offerors will be evaluated under these factors based on the following:

- Factor A: Technical Approach
- Factor B: Information Security
- Factor C: Staff Experience and Qualifications
- Factor D: Management Plan
- Factor E: Past Performance
- Factor F: Price

Basis for Award (Best Value)

The Center intends to evaluate proposals based on the evaluation criteria listed above and make award without discussions to the offerors. However, the Center reserves the right to conduct discussions if

later determined to be necessary. Therefore, each offer should contain the best terms from a cost or price and technical standpoint.

Award will be based on the combined evaluations of Technical, Past Performance, and Price. The contract resulting from this competition will be awarded to the responsible offeror whose offer, conforming to the requirements, is determined to provide the "best value" to the Center, which may not necessarily be the proposals offering the lowest price nor receiving the highest technical rating.

Although non-price factors, when combined, are significantly more important than price, price is an important factor and should be considered when preparing responsive offers (proposals).

When offerors are considered essentially equal in terms of non-price factors or when price is so significantly high as to diminish the value of the technical superiority to the Center, price may become the determining factor for contract award. In summary, price/non-price trade offs will be made, and the extent to which one may be sacrificed for the other is governed only by the tests of rationality and consistency with the established factors.

Proposal Description and Process

Participation in this RFP process is voluntary. All costs incurred in responding to, or in participating in this RFP, will be the responsibility of the vendors, or other third-party organizations participating in the RFP, and not that of the Center.

Confidentiality

Any document submitted in response to this RFP that contains confidential information must be marked by a watermark on the appropriate pages as “Confidential.” The confidential information must be clearly identifiable to the reader as confidential. All other information will not be treated as confidential. Note all confidential information is for the Center’s use evaluating proposals in response to this RFP.

Instruction and Response Guidelines

Responses to this RFP shall adhere to the page limits specified and must be in narrative form and provide details on vendor product capabilities. Responses must be viewable with Microsoft Word or Adobe Acrobat and printable on 8.5” x 11” paper, must use 12-point font, the margins of each page should be at least ½ inch, and each page should contain a page number in the footer.

Reponses must be received electronically by 5:00 p.m. Eastern Daylight Time on December 6, 2019. Responses will be sent to the email address of the sender along with any additional email addresses included in the submittal.

Please ensure that the submittal is in Microsoft Word or PDF format. All responses must be submitted electronically to the following email address: DataHubRFP@naswa.org

Telephone calls regarding this RFP will not be accepted. Questions may be submitted by email up to 5:00 p.m. Eastern Daylight Time, November 15, 2019. The Center will review post questions and answers to the RFP website.

Appendix A

SAR Lookup Suspicious Data Elements

IP Address : 250.250.250.211	Email : testing@test.com	Suspicious Email Domain : No
Address 1 : 111 S Main Salt Lake City UT 84111	Address 2 :	
Phone 1 : (555) 111-2233	Phone 2 : (655) 111-2233	Phone 3 :
Direct Deposit Routing Number : 021000021	Direct Deposit Account Number : 12121212	

SAR Lookup Match Result(s). Rows Returned - 5

20 (1 of 1)

State	Unique ID	IP Address	Email	Address 1	Address 2	Phone 1	Phone 2	Phone 3	Direct Deposit	Effective Date	Occurrence Date
California	000000000000CA1	MS				M			M	07/06/2018	09/10/2018
California	00000000ST1-099	MS				M			M	07/06/2017	09/10/2017
California	000011111111111	MS				M				07/06/2016	09/10/2016
California	0000000CA234987		MS							07/01/2018	08/01/2018
Oregon	00000000ST2-099						M		M	07/06/2015	09/10/2015

Figure 1: SAR-IDH Matching Report

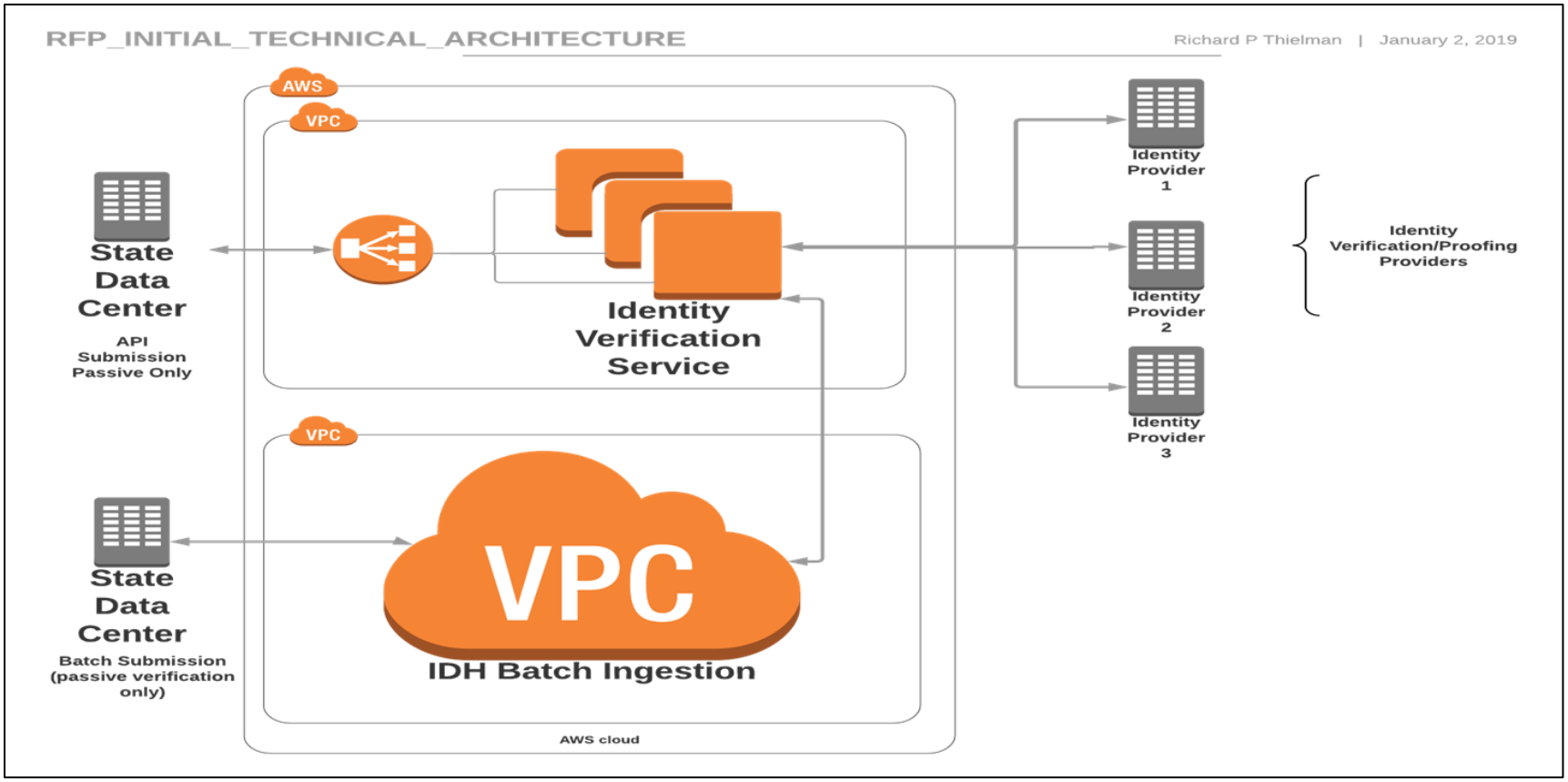


Figure 2: Identity Verification Service Architecture

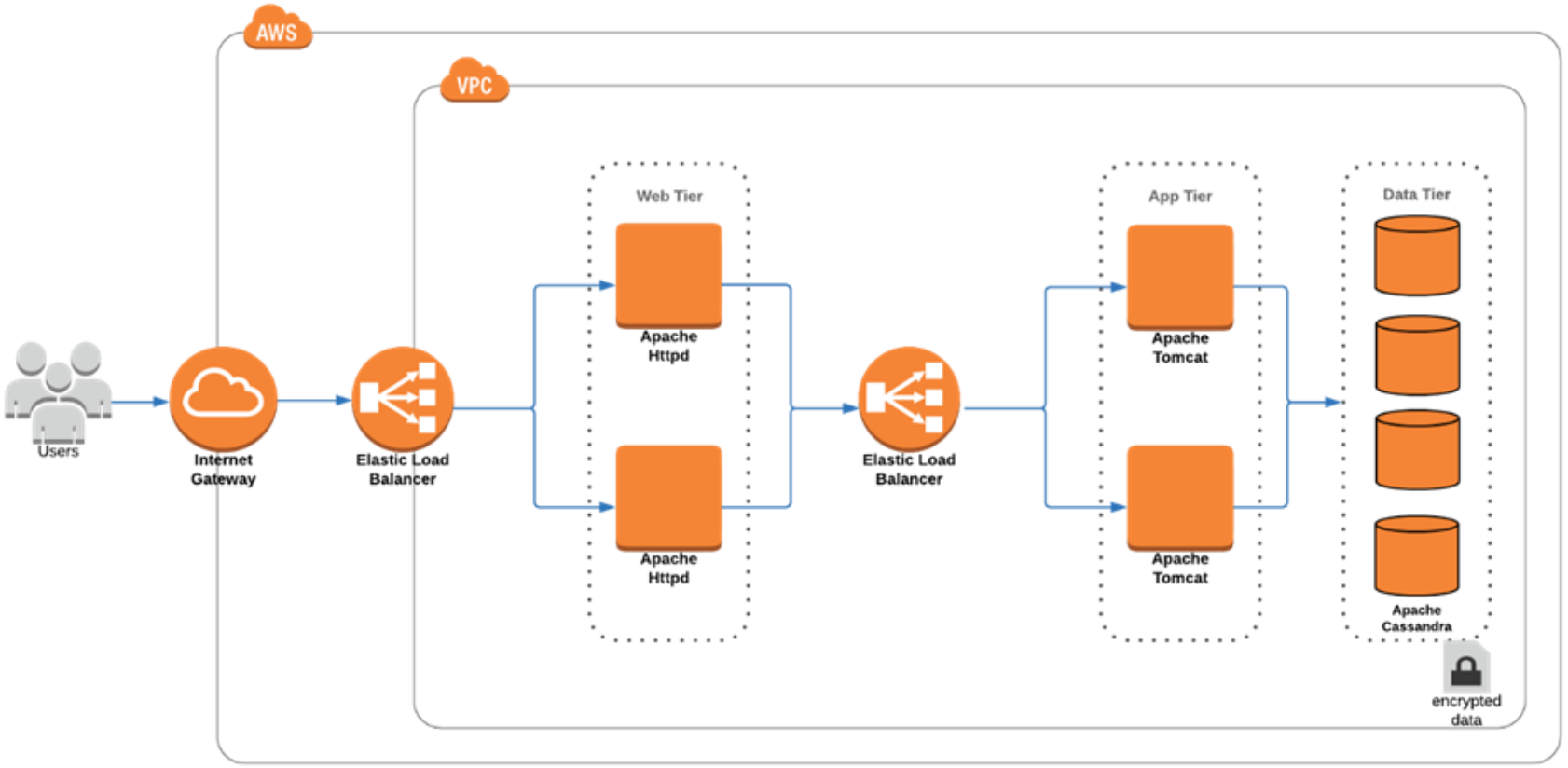


Figure 3: IDH Architecture