INTEGRITY

NASWA UI Integrity Center

In Partnership with USDOL

Request for Proposal

Centralized Account Verification Services (AVS)

November 5, 2020

Contents

Introduction

The Unemployment Insurance (UI) Integrity Center (Center) has been formed in partnership with the U.S. Department of Labor (USDOL), Employment and Training Administration (ETA) Office of Unemployment Insurance (OUI), the New York State Department of Labor (NYSDOL), and the National Association of State Workforce Agencies (NASWA) to provide innovative tools, training, and support to state workforce agencies (SWAs) in their efforts to reduce improper payments and combat fraud.[1] The Center's mission is to be a go-to resource for successful UI program integrity and improper payment reduction strategies and tools, focusing particularly on the prevention, detection, and recovery of improper payments. One of the Center's key initiatives is the development and state adoption of the UI Integrity Data Hub (IDH).

To ensure the integrity of UI programs, the Center developed a centralized IDH comprised of multiple databases for the purpose of identifying matches to state-submitted UI claims data. The originating states receive matches for further investigation and processing at their discretion. The IDH crossmatches help states identify new cases of potential fraud and otherwise undetected improper payments.

Currently the Center is seeking to define, develop, test, and implement a centralized bank account owner validation and verification service through the IDH for SWAs to use in their efforts to prevent UI fraud and improper payments. The Account Validation Service (AVS) will serve as an additional resource and provide new indicators via the IDH output for states to review, investigate, and verify UI claimant data.

Purpose of This RFP

The Center is currently working with USDOL to establish funding to provide a centralized AVS to address the need for SWA's to incorporate bank account owner verification into their UI claims process, leveraging the existing IDH infrastructure. As such, the Center is seeking a vendor to provide the Center with a software-as-a-service (SaaS) AVS capability. Final award of a contract with a selected vendor will depend on the Center securing the necessary funding from USDOL.

The Center is seeking a solution that will deliver a determination of the validity of a UI Claimant's bank account and routing number. Specifically, that the identity associated with a submitted UI claim matches the identity of the bank account owner/authorized signatory of the direct deposit bank account information provided (to include verification of pre-paid cards to the extent feasible). For this purpose, the Center is requesting responses from qualified vendors capable of utilizing their products and services to provide a response to the IDH to validate and verify a UI claimant's self-attested bank account information.

Reponses must be received electronically by 5:00 p.m. Eastern Standard Time on December 21, 2020 at DataHubRFP@naswa.org.

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

[1] https://wdr.doleta.gov/directives/attach/UIPL/UIPL_28_12_Acc.pdf

Background

Since 2010, the UI Program has had an improper payment rate around 10 percent or more. From January 1, 2019 to December 31, 2019, the most recent year for which data is available, the national improper payment rate as estimated by the UI Programs' Benefit Accuracy Measurement (BAM) was at 9.86 percent. This represents an estimated $2.6 billion in CY 2019 in improper payments nationally.[2] As a result of the tremendous increase in UI and Pandemic Unemployment Payments in CY 2020 the extent of fraudulent and overpayments is expected to be several magnitudes greater.

While there is no data specific to the UI program on the prevalence of bank account fraud, the Association for Financial Professionals *2020 Payments Fraud and Control Survey Report*[3] found that, "thirty-three percent of financial professionals report that their organizations' payments via Automated Clearing House (ACH) debits were subject to fraud attempts/attacks in 2019." Similarly, the report found that 22 percent of financial professionals reported fraud activity through ACH credits in 2019. The report cites that, "as fraudsters move away from targeting checks and wires, they are resorting to ACH transactions as vehicles for their scams. In efforts to avoid raising red flags and escape detection, perpetrators of such attacks are attempting to use payment methods previously not considered to be high risk." SWAs have dealt with this type of ACH fraud for several years as most states provide the ability for claimants to request benefit payments deposited directly into their bank account but again in CY 2020 the volume of fraud and the associated deposits in banks has significantly increased.

The USDOL Office of the Inspector General has identified fraudulent claims based on false identities and fraudulent bank account information as a top management challenge for the UI program. In addition, the enactment of the Coronavirus Aid, Relief, and Economic Security (CARES) Act UI programs has caused a significant spike in UI fraud and use of fraudulent bank account information. One of the integrity challenges SWAs face is the use of single bank accounts for the deposits of benefits for multiple claims.

Another challenge SWAs face is with "hijacked claims." This happens when a legitimate UI claimant files for benefits, but a fraud group hijacks the claim and changes the bank account information to intercept the UI benefits. With the tremendous increase in funds expended in regular UI programs and in the new programs created under the CARES Act of 2020, the volume of deposits initiated by states into the banking system is in the hundreds of billions of dollars. A significant amount of that funding flows to claimants' direct deposit accounts, and in some cases, is going to individuals who have provided fraudulent bank account information.

A properly functioning AVS tool will enable states, through the IDH, to validate the status and owner of bank accounts across the U.S. in real-time to provide increased fraud prevention prior to the distribution of benefit payments. It can be used to verify the status of an account and ownership prior to sending an ACH or real-time payment, checking to see if the account is open and in good standing, and that the benefit recipient is an owner, or authorized signer on the account. Data returned to the SWA will allow the SWA to determine whether the account is possibly a fraudulent account, or stolen account. The AVS has the goal of reducing the incidence of UI benefit payments being sent to bank accounts not associated with the true identity of the claimant filing for benefits.

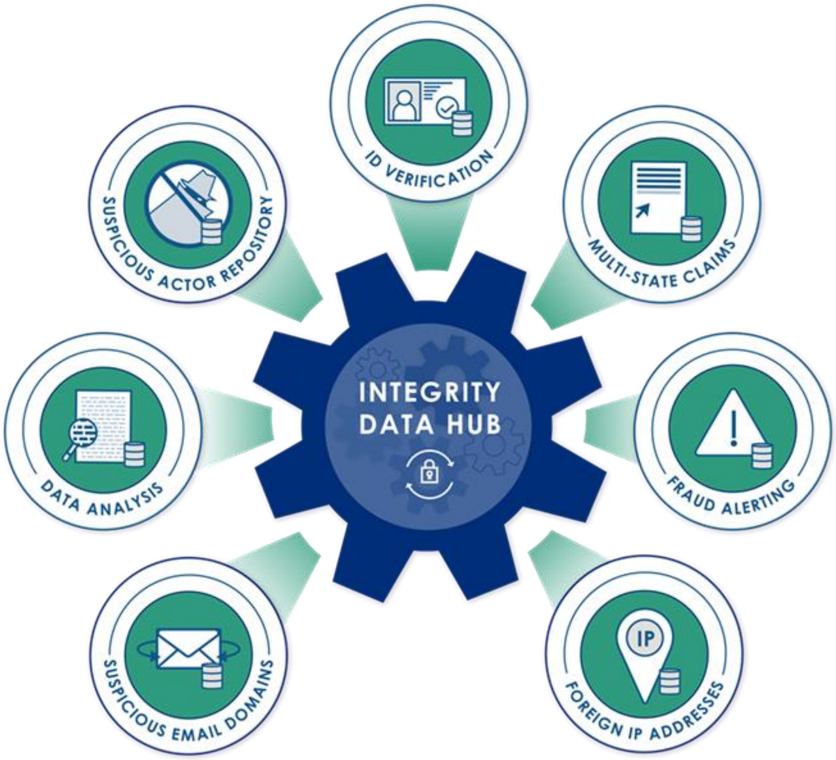
[2] https://www.dol.gov/general/maps/data
[3] https://www.jpmorgan.com/content/dam/jpm/commercial-banking/documents/fraud-protection/afp-fraud-survey-2020-report-highlights.pdf

Integrity Data Hub

The IDH is a secure, centralized multi-state data tool which allows participating SWAs to submit claims for analysis and crossmatching against multiple data sources. Participating SWAs 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 IDH website or spreadsheet upload. More automated channels such as secure FTP (sFTP) and web services are available.

Data elements provided on UI claims sent to the IDH are crossmatched against the different data sources and services, both internal to NASWA and held by external agencies. The system generates a report back to the submitting state containing the matched data elements and other scoring information for further investigation and review by the submitting SWA. The IDH contains an increasingly expanding set of data sources to provide data crossmatching and analytic capabilities. The Center continues to develop and enhance the IDH, with a goal of maximizing state involvement by providing a service that SWAs fully trust and regard as a valuable tool. Summarized below and illustrated in Figure 1 are the primary databases housed in the IDH and services provided by vendors through the IDH to help states identify potential UI fraud and improper payments.

Figure 11: UI Integrity Data Hub Databases



Suspicious Actor Repository (SAR) –The purpose of the SAR is to collect suspicious actor information from participating states into a master file for use by states in accordance with their respective UI integrity policies and business rules. Participating states match current claims against this state-populated database of fraudulent and suspicious claims data. The repository leverages the investigative power of all states for the benefit of each state.

Foreign IP Detection – The Foreign IP Detection database allows states to have claims submitted from outside the United States undergo additional review and scrutiny. States who include the IP address of claims filed can use the IDH to determine whether the claims are suspect and may be fraudulent.

Multi-State Crossmatch (MSCM) – The Multi-State Crossmatch is a data source that allows participating states to determine if data elements on a claim filed in their own state match on claims in other IDH participating states. The MSCM stores all claims data submitted by states for crossmatching into a secure database.

Fraud Alerting – The IDH makes available a secure communication platform that allows participating states to notify each other of emerging fraud schemes and trends discovered in their states. Registered users receive email notifications when Fraud Alerts and created and updated. This allows states to communicate in a systematic manner, so they can look for similar fraud schemes within their own system and prevent fraudulent claims.

Identity Verification – The Identity Verification (IDV) crossmatch provides identity verification services to all states participating in the IDH. The IDH provides a centralized identity verification solution integrated with Experian Information Solution's (Experian) Precise ID identity verification platform that allows states to submit claimant information included on UI claims[4] to verify and validate the identity in use by the claimants. The IDV crossmatch assists states in determining that those individuals filing for UI benefits are indeed the person they say they are and prevent fraudulent claims filed with stolen identities.

Account Verification Functionality Objective

The Center is currently working with participating SWAs to collect weekly UI Initial and Continued UI claims data. The IDH serves as a centralized data repository and will transmit each SWAs data to the AVS vendor at regular intervals using real-time webservice 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 AVS solution will provide SWAs with the assurance that the UI claimant is an authorized signatory on the bank account to which UI benefits are to be disbursed. The AVS vendor will execute bank account ownership validation and verification against this claims data and provide the results back to the IDH including a set of bank account validity and ownership indicators.

Upon completion of the account validation and verification analysis, all claims data transmitted to the AVS vendor will be permanently and verifiably deleted and not stored by the vendor in any fashion.

The AVS solution is expected to function in a solely passive fashion, without a need for direct claimant interaction with the AVS vendor. No "out of pocket" or "out of wallet" information will be requested of the claimant. Additionally, claimants will not be requested to provide their online bank account information or credentials to login, to verify account ownership.

[4] States can send all claim types to the IDV solution including initial, additional, reopen, and manual.

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 bank account and/or UI improper payment fraud. These datasets will provide SWAs access to: (1) real-time claimant bank account owner verification and bank account risk assessments, and (2) risk attributes associated with the account owner analysis.

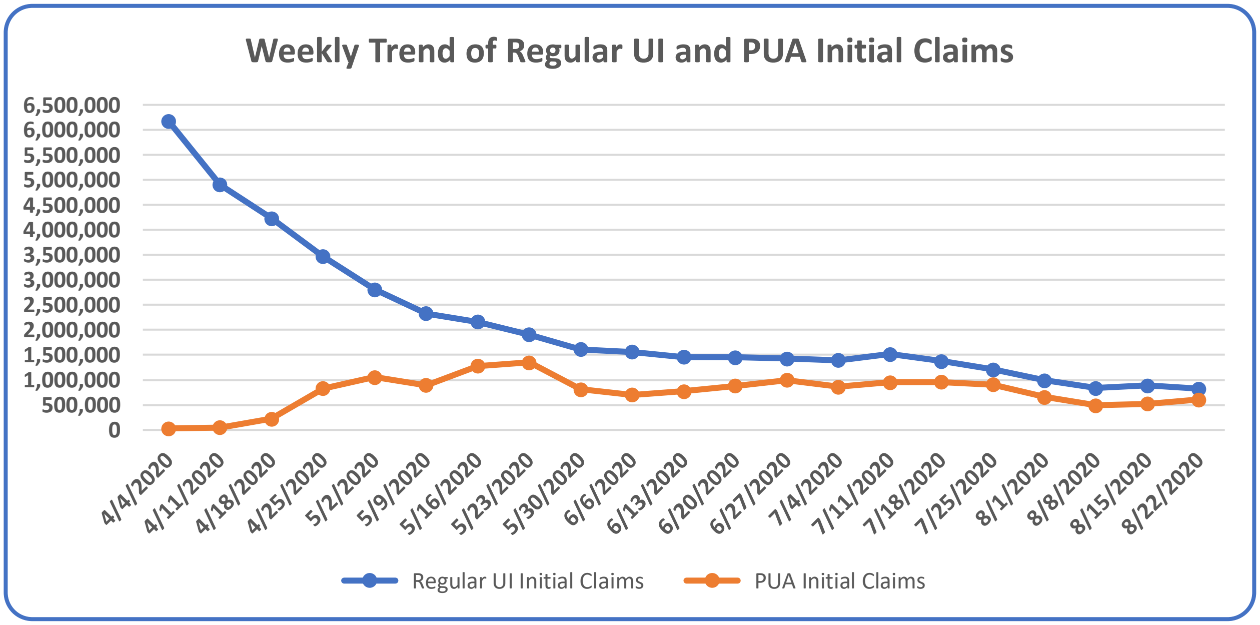
The Center's AVS service is expected to function as an augmentation of the current IDH, and minimally impact the SWA-specific processes for handling electronic UI claims already in place. This augmentation is currently envisioned as an additional set of indicators returned in an expanded IDH Matching Report for each submitted claim. The current matching report format is shown in Appendix A Figure 1.

The AVS architecture utilizes a micro-service based open source software stack in an AWS cloud-based environment according to NIST based best practices as shown in Appendix A Figure 2. The open source stack currently includes Red Hat Linux, Apache Httpd, Apache Tomcat, Apache Cassandra, and MySQL RDS. OpenAM and OpenDJ are used for single sign on. The AWS cloud-based environment provides scalability, flexibility, availability and ease of management. There will be an AWS ECS cluster which provides an AVS microservice to our internal applications. This microservice will directly connect to the vendor AVS API through a secure AWS connection or VPN. The microservice may scale automatically based upon incoming bursts of traffic.

UI IDH Transaction Volume

The volume of AVS requests is dependent on the number of initial UI claims filed and utilization for the IDH by SWAs and will increase or decrease depending on: the extension of temporary UI programs, the level of economic activity and the extent of SWA participation. Current volume could possibly be approximately 2 million verification requests per week if all SWAs participated and the current unemployment rate and economic conditions are sustained. The overall trend resulting from the COVID-19 Pandemic is displayed in Figure 3 from April 2020 through August 2020, but it may not represent future activity.

Figure 3: Initial Claims of Regular UI and PUA Programs



Current volume is not necessarily indicative of future volume. Transaction volume will not be consistent but come in bursts of traffic which can spike due to time of the day, economic conditions, state on-boarding, or state feature selection. The vendor solution should scale or be provisioned to handle this use case.

Anticipated Solution

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

1. Passive claimant bank account validation and owner verification shall be delivered from the data elements defined below. Passive is defined as verification completed from data transmitted by the IDH to the AVS vendor for validation and 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 solution shall not require claimants to provide online banking login credentials to verify account ownership.

   The claims data elements transmitted to the IDH by states and available to the AVS solution include the following:

Date Field	Comments
State code	2-digit postal code of submitting state
Claimant address	If data in Claimant address, data for city, state, and zip is
Claimant address city	City of Claimant address
Claimant address state	State of Claimant address
Claimant address zip	Left justify if less than 9 characters
Claimant phone number	Phone number provided by clamant
Direct Deposit Account Number	Direct deposit account number for payment to Claimant
Direct Deposit Routing Number	Routing number associated with above account number
IP Address	IP address from where claim was filed
Claimant Email	Email address provided by claimant
Claim Effective Date	Effective date of claim filed
Claim Occurrence Date	Date suspicious activity started
First Name	Claimant first name
Last Name	Claimant last name
Middle I	Claimant middle initial
SSN	Claimant SSN

Date Field	Comments
DOB	Claimant date of birth
Claim Type	Initial, Continued, Re-open, Additional
Program Type	UI, PUA, PEUC, TRA, EB

2. Process individual requests via API.
3. Information used to evaluate the bank account validity and account ownership may be matched through multiple sources of data to increase the accuracy of the evaluation and decrease the likelihood of false positives and false negatives. This information could also allow the SWAs to understand and have indicators to know when there are multiple account owners associated with a bank account submitted to the AVS.
4. The solution should have the widest reach possible. Vendors should specify in their proposal the estimated percentage of all bank accounts covered by their solution.
5. Vendors should specify in their proposal estimated accuracy measure of their solution.

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 AVS data service deliverables and establish the schedule for the AVS' implementation of AVS 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 AVS solution, in coordination with the IDH project team, to include functional and load testing to ensure the AVS 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.
6. 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 AVS 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 AVS responses to the IDH.
7. Compliance with all laws and regulations under the Gramm-Leach-Bliley Act (GLB), Fair Credit Reporting Act (FCRA), NACHA rules and regulations, and other applicable state statutes.
8. Solution must operate as webservice API with a maximum transaction time of 100ms.
9. Solution must handle bursts of webservice traffic without performance degradation.
10. Solution must incorporate the highest levels of security to protect claimant PII.
11. Solution should provide mechanism for a secure direct connection from IDH through AWS cloud or VPN to the AVS vendor data center.
12. Solution be pass-thru with respect to IDH data or should not store IDH data beyond timeframe where it is needed to process each AVS request.

13. Solution should have high availability with redundancy to maximize uptime to highest degree possible bound by vendor Service Level Agreement (SLA).
14. Vendor must provide effective mechanism for technical support for any system issues or outages post go-live.

Restrictions Against Disclosure

The Vendor implementation of the AVS 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 IDH shall be permanently deleted by the Vendor in a verifiable fashion upon completion of the AVS 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 AVS 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[5]. 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 AVS purposes is purged from the system following processing

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

- 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 AVS 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
        - 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 AVS 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 estimated timeline of RFP-related events:

RFP Activity	Estimated Timeline
AVS RFP Webinar*	Dec 1, 2020
Final Clarification Questions	Dec 8, 2020
Questions and Responses Posted	Dec 11, 2020
Proposals Due	Dec 21, 2020
Offeror Presentations**	Week of Jan 11, 2021
Best and Final Offer Pricing (optional)	Jan 22, 2021
Award (anticipated)	Feb 2021

* 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/RFP_AVS.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 will be conducted virtually via NASWA-organized ZOOM meetings.

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
Initial connectivity test	Award +60 days
State pilot testing	Award +90 days
Production solution available	Award +120 days

Period of Performance

The Period of Performance for this procurement is anticipated to be 36 months from the date of the execution of the contract. Contingent on funding from USDOL. 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	SECTION	FORMAT	PAGE LIMIT
Factor A	Technical Approach	Written	20 pages total
Factor B	System and Data Security	Written	20 pages total
Factor C	Staff Experience and Qualifications	Written	10 pages total

PART II BUSINESS	SECTION	FORMAT	PAGE LIMIT
Factor D	Past Performance	Written	3 References, 6 pages total
Factor E	Management Plan	Written	8 pages total
Factor F	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 AVS project in a manner that will provide the Center with cost effective and quality services.

1. Bank Account Validation and Verification Service:
   - Data transmission methods and associated API formats for interfacing with the IDH;
   - Rubric for evaluation data returned to the IDH (with examples);
   - Additional flags/information returned for state investigation, on a per claimant bank account basis (with examples);
   - Provide configuration capability for returned indicators to be included in the expanded IDH Match Report (Appendix A Figure 1) returned to the SWAs;
   - Provide accuracy rate for validation and verification of bank account validity and owner verification, including false positive rate;
   - Provide appropriate utilization rate of the validated and verified bank account owner information, including false negative rate;
   - Provide AVS processing rate, including volume and concurrent request capacity rate;
   - Provide AVS national and state level banked population coverage (i.e. how much of total bank accounts at state and national level does AVS service have access to validate and verify ownership);
   - Provide description of ability to access bank account deposit information and transactions to detect potential unreported income by claimants;
   - Provide details on AVS system architecture including but not limited to security, scalability, availability, redundancy. Example but not ideal architecture is shown in Appendix A Figure 2;
   - Provide API interface documentation with details including but not limited to minimum necessary fields required, optional but desired fields, vendor unique identifier for each request, along with AVS request and response details and security;

- Provide vendor AVS system SLA transaction and response times for AVS requests along with any volume or concurrent request constraints, if any; and
- Provide details on scalability to of AVS architecture ability to handle bursts of traffic or concurrent requests.

2. Information security:
   - Provide indication data storage policy of pass-thru system without IDH data storage and/or verifiable deletion of all IDH provided data upon AVS request completion;
   - Provide data encryption specification and strategy for all IDH provided data, both at rest and in motion;
   - Provide disclosure of data use policy that IDH data will not be used for any other purpose other than AVS for support or processing the specific AVS request;
   - Provide AVS vendor API security architecture; and
   - Provide security specifications and details on available connections through AWS cloud or VPN to the AVS vendor data center with regard to performance, configuration, and encryption standards.

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 bank account validation and owner verification;
   - 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 bank account validation and owner verification;
   - Provide details on the implementation process with respect to the SDLC and test and production AVS system capability and process;
   - Provide description for preferred methods of the following for implementation:
     - Requirements gathering;
     - Solution integration with AVS partner;
     - Testing and verification methodologies;
     - Estimating implementation timeline post requirements finalization; and
   - Ongoing communications with the UI Integrity Center project manager and project team.

5. Post-Implementation Support:
   - Provide details on vendor SLA technical support that will be provided post go-live including but not limited to response and resolution times for issue severity and Points of Contact (POCs);
   - Provide vendor SLA for system transaction time, reliability, and availability; and
   - The Center intends to include in the contract with the selected AVS vendor provisions to validate both acceptable technical performance (ex. transaction times within SLA levels) and acceptable post implementation support (ex. response times in resolving user/production issues).

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 AVS 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.

The Center is interested in evaluating the cost/benefit of varying levels of service and data sources used for AVS. As such, If the offerors solution includes varying/optional tiers of service, data sources, and/or AVS, 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.

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 Approach, 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 tradeoffs 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.

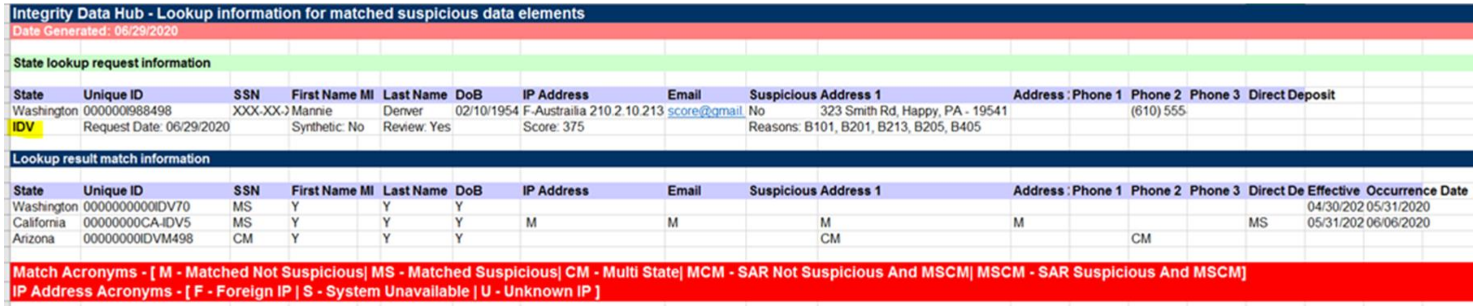
Instruction and Response Guidelines

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 21, 2020 at DataHubRFP@naswa.org. Acknowledgement emails will be sent to the email address of the sender along with any additional email addresses included in the submittal.

Telephone calls regarding this RFP will not be accepted. Questions may be submitted by email up to 5:00 p.m. Eastern Daylight Time, December 8, 2020 at DataHubRFP@naswa.org. The Center will review post questions and answers to the RFP website.

Appendix A



Integrity Data Hub - Lookup information for matched suspicious data elements

Date Generated: 06/29/2020

State lookup request information

State	Unique ID	SSN	First Name MI	Last Name	DoB	IP Address	Email	Suspicious	Address 1	Address :	Phone 1	Phone 2	Phone 3	Direct Deposit
Washington	000000I988498	XXX-XX-)	Mannie	Denver	02/10/1954	F-Austrailia 210.2.10.213	score@gmail.	No	323 Smith Rd, Happy, PA - 19541			(610) 555-		
IDV	Request Date: 06/29/2020		Synthetic: No	Review: Yes		Score: 375		Reasons: B101, B201, B213, B205, B405						

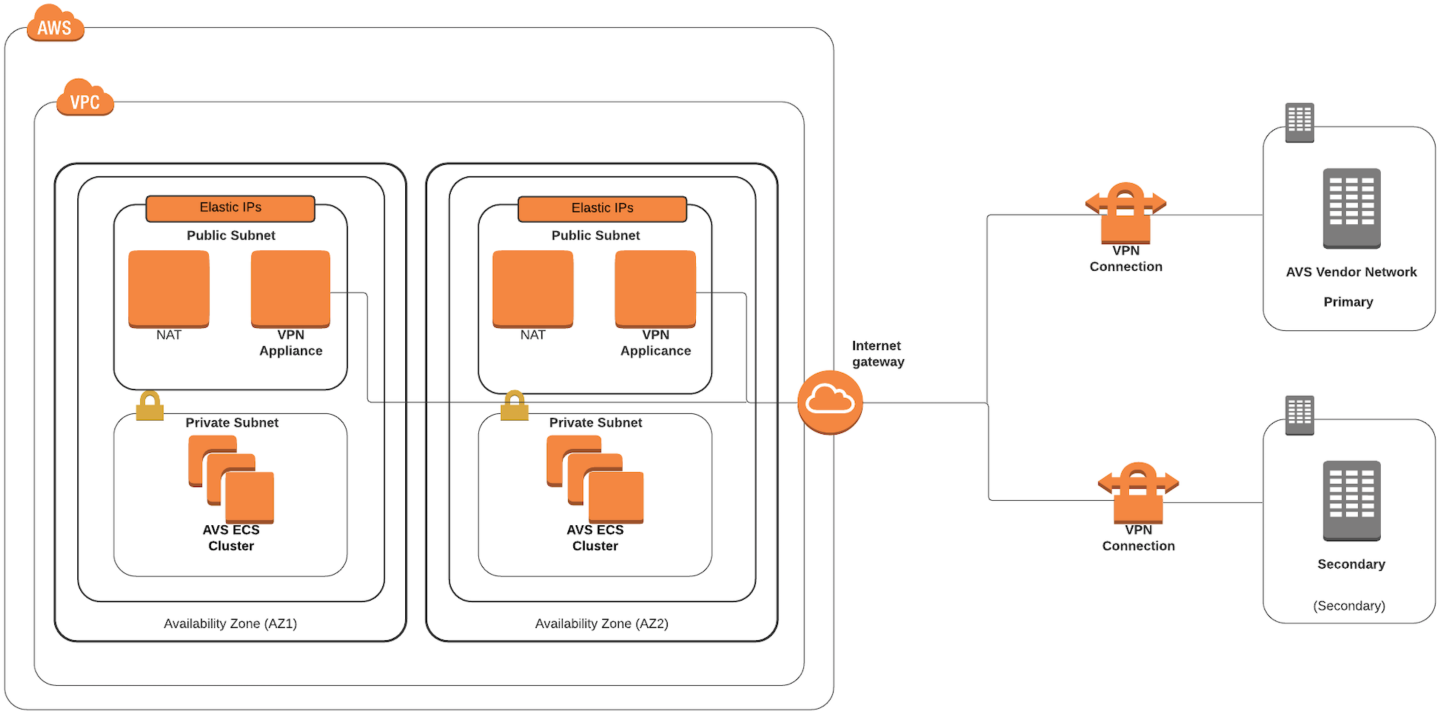
Lookup result match information

State	Unique ID	SSN	First Name MI	Last Name	DoB	IP Address	Email	Suspicious	Address 1	Address :	Phone 1	Phone 2	Phone 3	Direct De	Effective	Occurrence Date
Washington	0000000000IDV70	MS	Y	Y	Y										04/30/202	05/31/2020
California	00000000CA-IDV5	MS	Y	Y	Y	M	M		M	M				MS	05/31/202	06/06/2020
Arizona	00000000IDVM498	CM	Y	Y	Y				CM			CM				

Match Acronyms - [M - Matched Not Suspicious| MS - Matched Suspicious| CM - Multi State| MCM - SAR Not Suspicious And MSCM| MSCM - SAR Suspicious And MSCM]

IP Address Acronyms - [F - Foreign IP | S - System Unavailable | U - Unknown IP]

Appendix A Figure 1: IDH Matching Report



Appendix A Figure 2: Option for On-Premise Vendor Integration with Redundant Legacy VPN (Appliance Instead of AWS Managed VPN)

***AWS 2 AWS solution or AWS Managed VPN to on-premise will vary.**