**General Services Administration**

Federal Acquisition Service  
National Capital Region and

Technology Transformation Services

1800 F St NW | Washington, DC | 20006

**Login.gov Identity Proofing**

DRAFT

Statement of Work

# Introduction

This document represents a Statement of Work (SOW) to acquire products or services for the General Services Administration (GSA), Technology Transformation Service (TTS) login.gov Program. login.gov is a growing platform and needs a variety of proofing methods, data sources in order to move towards the goal of universal coverage for the U.S population. As login.gov grows there is the need to have the mix of methods/data sources that can most effectively proof login.gov’s partner agencies populations. The intent with a multi-award contract is to provide a broad base of contractors who the government can work with to have the highest proofing rate for an agency population. Each order will help support different population subsets and the data from those order will inform our planned proofing rate vs actual and allow for iterating. Note underserved in this context is being defined as “The underserved are a geographically, economically, and demographically diverse group of people who, by choice or circumstance, operate partially or completely outside the traditional banking system.”

# Identity Resolution

The goal of identity resolution is to uniquely distinguish an individual within a given population or context. Effective identity resolution uses the smallest set of attributes necessary to resolve to a unique individual. In order to effectively demonstrate proofing Contractors must be able to resolve 50% of the U.S population or provide a compelling case for providing service for a traditionally underserved demographic. Able to return validation and values for the attributes listed under LOA 3 at this link <https://developers.login.gov/attributes/> except UUID and email address.

# Address Verification

Ability to confirm an address of record that must include at a minimum phone number or postal address and tying it to a person’s identity for the U.S population. At a minimum be able to identify 10% of the U.S population or provide a compelling case for providing service for a traditionally underserved demographic.

# Account Verification

Ability to electronically tie a user to an account in a way that supports NIST 800-63-3A Fair evidence for Identity Assurance Level 2 <https://pages.nist.gov/800-63-3/sp800-63a.html>. Examples of this include but are not limited to utility accounts, financial (depository, non-depository), other recurring activities such as rent payments, monthly deposits or payments, other methods. At a minimum be able to verify 10% of the U.S population or provide a compelling case for providing service for a traditionally underserved demographic.

# Behavioral Analytics

Ability to apply behavioral analytic techniques including the ability to monitor identities over multiple dimensions such as time, geolocation, pattern of use, attribute changes for indicators of potential fraud and provide that back to login.gov as indicators. Utilizing data points such as these attributes <https://developers.login.gov/attributes/>, device fingerprints, IP Address.

# Government ID Verification

Validate the government identity documents with issuing and/or authoritative sources to confirm there is a corresponding electronic record. An example is validating the information from a state id with the state that issued it.

# General Requirements

|  |  |  |
| --- | --- | --- |
| **ID** | **Requirement** | **Priority** |
|  | Provide a population breakout of U.S population coverage by household income, age, geography (postal code) | Mandatory |
|  | Ability to provide response via Application Programming Interface (API). | Mandatory |
|  | Offering is an existing commercial software product not new custom developed for this contract | Mandatory |
|  | Provide a monthly status report or access to a real time dashboard with summary level data | Mandatory |
|  | Ability to provide a maintenance schedule detailing any infrastructure, software or data updates and upgrades, duration, impact on login.Gov, expected downtime etc. | Mandatory |
|  | Log points of failure and provide regular reports on that. | Mandatory |
|  | Ability to export all reports and transactional logs in .CSV format. | Mandatory |
|  | Support for English language. | Mandatory |
|  | Support for other languages including but not limited to Spanish and French. | Not Mandatory |
|  | Contractor identity solutions comply with Section 508 Requirements. | Mandatory |
|  | Ability to provide detailed raw log information regarding system events, transactions, in a standard format (such as .CSV, pipe, line delimited) with standardized delivery to be determined mutually with the Government. | Mandatory |
|  | Maintain test environments to allow for separation of real test data with the ability for the Government to conduct end-to-end testing that are a mirror of production. | Mandatory |

## 6.1 Technical Support

GSA requires ongoing technical support in the event of planned/unplanned system failures and to resolve performance issues. The Contractor must:

* Provide GSA with a technical Help Desk Contact telephone number that can be accessed by GSA personnel in need of technical support.
* Provide production support for issue resolution 24 hours per day, seven (7) days per week, 365 days per year. Contact Person(s) must be capable of resolving issues related to system failures and system under-performance.
* Provide GSA with service interruption procedures and a service recovery plan that reflects service restoration Service Levels.
* Provide support for any confirmed or suspected incident investigations.
* Once login.gov integration goes live, participate in periodic reviews of proofing pass/fail rates and other performance metrics, and tuning exercises in order to improve proofing rates. This will involve the analysis of system configuration, reports, creation of recommendations to improve the results and the underlying identity model, actual changes to the system and the Identity model(s) and supporting structure.
* Provide access to technical support personnel during configuration, validation, and testing of the web service as agreed to in the Implementation Plan.

## 6.2 Service Level Requirements (SLRs) – Production Environment

GSA requires a software solution that is highly available and provides business-class response time. The Contractor must:

* Perform constant monitoring of systems availability and alert GSA (via a method mutually agreed by GSA and Contractor after contract award) in the event of service interruption support within 15 minutes of service interruption:
  + To the extent possible, alerts must include the start time of the outage, effect of the outage (i.e., are all customers affected, or only some States/Jurisdictions), the suspected cause of the problem (if known), and steps being taken to resolve the outage.
  + Once the outage is resolved, the Contractor must send a closing alert to GSA. This communication must include the end time of the outage, the duration of the outage, the effect of the outage, the number of transactions affected by the outage (if known), the actual cause of the problem and the steps planned to prevent similar outages in the future.
  + Contractor shall measure and report response times for both the individual Jurisdictions and the Contractor’s own system on a monthly basis. In the event the SLA is not met the Contractor shall report to the Government where the issue is.
  + Security incidents with potential impact to availability, confidentiality, or integrity must be immediately reported but not more than one (1) hour following detection to the GSA TTS Contracting Officer (CO) or the Contracting Officer’s Representative (COR) and the General Services Administration Incident Response Team. Maintain 24x7 monitoring with geographically dispersed disaster recovery capabilities.
* Provide notification of scheduled systems downtime to GSA one (1) month prior to the planned service interruption.
* Comply with the service level requirements defined in this section for availability, system response time, capacity, security, and incident reporting.

### 6.2.1 Contract Closeout Plan

The Contractor must also establish and implement plans for an orderly phase out of operations at the termination of this contract that ensures data security and integrity while data is in transit.

## 

#### Performance Management Metrics

On a monthly basis, the Contractor must meet the performance objectives listed in the table below. Any deliverable(s) or non-performing service(s) that do not meet the Performance Measure and associated Inspection and Acceptance Criteria must be repaired/replace/re- performed by the Contractor.

|  |  |
| --- | --- |
| **Performance Requirement** | A specific task to be completed or deliverable to be furnished |
| **Performance Standard** | Standard represents the performance baseline against which the Contractor will be measured. |
| **Performance Surveillance** | The method used to measure the Contractor’s performance methodology (source, or data collection method) |

|  |  |  |
| --- | --- | --- |
| **Performance Requirement** | **Performance Standard** | **Performance Surveillance** |
| Service Availability | Available 99.9% of the total minutes in each calendar month. | 100% Inspection of Reports |
| Unavailability Notification | The Contractor must notify the COR and login.Gov PMO within 15 minutes of any service unavailability in order to coordinate consumer help desk messaging and support to consumers. | 100% Inspection of Reports |
| Scheduled Outages | Must not exceed a maximum of four (4) consecutive hours. | 100% Inspection of Reports |
| API Response Time | Fewer than 1000ms 95% of the time during a calendar month at service level and overall service level (under the identity service’s control). | 100% Inspection of Reports |
| Delivery of contract deliverables | Clarity, accuracy and contains all data required. Initial deliverable submission must be 90% error free. | 100% Inspection of Reports |
| Recovery Time Objective | Less than or equal to 30 minutes from a triggering incident occurrence. | Post Recovery Analysis |
| Recovery Point Objective | Less than or equal to 15 minutes from a triggering incident occurrence. | Post Recovery Analysis |
| Minimum Capacity after a Recovery Event | 33% of full operational capacity as specified in scalability requirements. | Post Recovery Analysis |
| Backup Data Retention Schedule | Daily backups retained for 7 days minimum.  Weekly backups retained for one month minimum.  Monthly backups retained for one year minimum.  Annual backups retained indefinitely. | Inspection of Backups |
| Maximum Time to Restore | 100% of operational capacity after a recovery event.  6 hours after reaching recovery time objective. | Post Recovery Analysis |
| Maximum Time for Data Restoration from Backup | 6 hours after request. | Post Recovery Analysis |
| Data Recovery Redundancy | Data and systems must be recoverable in a way that can survive broad regional disasters, through significant geographic distribution of operational and data storage facilities. | Assessment of continuity of operations plans, service and storage locations |
| Security Vulnerability Remediation | Standard patching is on a monthly schedule. Emergency patches are deployed for critical or high vulnerabilities known to be exploitable that do not have mitigating controls in place.  Security vulnerabilities must be corrected within specified time periods depending on severity:  Standard Patching:   * Critical - 30 Day * High - 30 Days * Medium - 60 Days * Low - 90 days   Emergency Patching:   * Critical - 1 Day * High - 1 Days | Post Remediation Analysis |
| Security Incident Reporting | Security incidents with potential impact to availability, confidentiality, or integrity must be immediately reported but not more than one (1) hour following detection. Incidents are reported to the GSA TTS Contracting Officer (CO) or the Contracting Officer’s Representative (COR) and the General Services Administration Incident Response Team. | 100% Inspection of Report |

* Provide a monthly outage report within ten (10) business days after the end of the reporting period, that includes the following information for each incident that occurred:

|  |  |
| --- | --- |
| **Title** | **Description** |
| Date | Date(s) the outage occurred. |
| Start Time | Time the outage began. |
| End Time | Time the outage ended. |
| Total Outage | Total number of hours, minutes and seconds the service was not working. |
| Description | Explanation of the problem that caused the outage. |
| Resolution | Steps taken to resolve the outage. |
| States | Number of States/Jurisdictions impacted by the outage. |
| Transaction | Number of transactions affected by the outage (when available); for example if the Contractor contractor was able to receive incoming transactions during the outage, but not transmit outgoing transactions, then the outage report should include the number of transactions received but not transmitted. |

#### Incident Management Standards

##### Problem Severity Guidelines

The vendor will respond to and resolve severity level 1, 2, 3 and 4 events within the timeframes set forth in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity Level** | **Characteristics** | **Recovery Time** | **Response Time** |
| **1** Severe business impact | * critical system, network, or key application outage with critical impact on service delivery * total loss of production service to entire customer set * impacts one or more service level commitments * revenue or delivery schedule impact * reassignment must be communicated / agreed directly | 2 hours (7/24 hours) | 1 hour |
| **2** Major business impact | * key component, application, critical end user machine or network is down, degraded, or unusable. Potential critical impact on service delivery * service performance degradation; service delivery impacted * partial customer set affected | 8 hours (7/24 hours) | 2 hours |
| **3** Minor business impact | * a component, minor application or procedure is down, degraded, or difficult to use. Some operational impact, but no immediate impact on service delivery * service outage, but alternative workaround available * potential exposure to delivery of service * scattered customers affected | 48 hours | 8 hours |
| **4** Minimal or no business impact | * component, procedure, not critical to customer is unusable. Alternative is available; deferred maintenance is acceptable * no impact to service * no production affected * individual customer affected | 10 days | 24 hours |

## 6.3 Security

* + - The software solution must:
* Provide a secure channel for real time data transmission between GSA and the Contractor. Integration testing must include review and validation of the web services connection including usage of secure protocols (e.g., TLS 1.2); FIPS-approved algorithms; and, FIPS 140-2 validated encryption modules. As per OMB Memorandum M-15-13, web site connections (if any) must use of HTTPS-only.
* Be in compliance with Federal standards and guidelines including:
  + FIPS 140-2: Encryption for backend data verification calls
* Provide data exchange in compliance with NIST encryption standards including usage of FIPS-approved algorithms, FIPS 140-2 validated encryption modules, secure Transport protocols, and secure key/certificate management.
  + - Contact information for GSA security POCs will be defined in the login.gov incident response plan.
    - The solution must be located in the United States. “United States” means the 50 States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, American Samoa, Guam, the U.S. Virgin Islands, Johnston Island, Wake Island, and Outer Continental Shelf Lands as defined in the Outer Continental Shelf Lands Act (43 U.S.C. 1331, et seq.), but does not include any other place subject to U.S. jurisdiction or any U.S. base or possession within a foreign country (29 CFR 4.112).
    - Despite enhanced security controls and monitoring, incidents may occur that require immediate response from the Contractor. Incidents could include misuse, fraud, misappropriation, espionage, sabotage, and inadvertent or deliberate compromise of the shared authentication platform. The Contractor must identify proposed plans, communications and protocols for responding to security and privacy incidents in collaboration with the Government. The Contractor must comply with incident reporting requirements outlined in GSA IT Security Procedural Guide 01-02, *Incident Response*.
    - Upon termination or expiration of the contract and upon request, once all data is provided back to the Federal Government the Contractor must discard all Government data within 7 years, and must certify no Government data has been retained unless otherwise authorized.
    - The Government will retain unrestricted rights to Government data. The data must be available to the Government upon request within one business day or within the timeframe specified otherwise in the Government’s request, and must not be used for any other purpose other than that specified herein. The Contractor must provide requested data at no additional cost to the Government.
    - No data related to the work under this contract must be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.
    - The Contractor must not disclose sensitive or proprietary information pertaining to GSA TTS or any of its operating units, the U.S. Government, industry, business partners, or consumers to any unauthorized persons. The Contractor must be subject to any and all penalties imposed by law for unlawful disclosure of sensitive information.
    - The Contractor must immediately notify, in writing, GSA TTS upon discovery of any inadvertent or deliberate disclosures of information other than those pursuant to performing the work under the contract. The Contractor must work with GSA TTS and make available its resources to work with GSA TTS and other entities to resolve this issue.
    - The Contractor must retain any PII consent logs created pursuant to this contract and transfer the logs to GSA TTS at the expiration of the contract.

#### Audit

1. Upon request from the COR the Contractor must allow the Government to perform manual or automated audits, scans, reviews, or other inspections of the contractor’s IT environment being used to provide or facilitate services for the Government. The Contractor must be responsible for the following privacy and security safeguards:

* To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor must afford the Government access to the Contractor’s facilities, installations, technical capabilities, operations, documentation, records, and databases within five business days of the request.
* Access to support incident investigations, must be provided as soon as possible but not longer than 72 hours after request.
* Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

1. The program of inspection must include, but is not limited to:

* Authenticated and unauthenticated operating system/network vulnerability scans
* Authenticated and unauthenticated web application vulnerability scans
* Authenticated and unauthenticated database application vulnerability scans
* Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the contractor chooses to run its own automated scans or audits, results from these scans may at the Government’s discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration must be approved by the Government. In addition, the results of contractor-conducted scans must be provided in full to the Government.

1. If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer must immediately bring the situation to the attention of the other party.
2. Upon request from the COR the Contractor must allow GSA TTS to conduct operational and security audits to verify the Contractor's compliance with our SLAs and security standards. The audits will be conducted following these guidelines:

​

* GSA TTS may perform one audit yearly, and may conduct additional audits after a confirmed security breach (one audit per breach). The Contractor must accommodate assessments by GSA TTS when requested. Unannounced assessments are required to occur within thirty business days from initial notification.
* The Contractor must make a good-faith effort to answer any questions GSA TTS has, and to give access to requested information (under suitable non-disclosure agreements (NDAs), if necessary). The Contractor must provide up to 40 hours of staff time per audit; any further time is at the Contractor’s discretion and may be billed at the Contractor's professional services rate.
* Any issues discovered by the audit must be remediated by the Contractor in a mutually-agreed-upon timeframe. High risk findings must be remediated within 30 days, moderate risk findings within 90 days, and low risk findings no longer than 180 days; risk levels are derived from the automated vulnerability scan tools based on [CVSS base scores.](https://nvd.nist.gov/vuln-metrics/cvss)

​

1. The Contractor must provide GSA TTS with any applicable documentation of their security stance and compliance achievements. Examples include:

​

* Internal security architecture documentation
* Internal security policies and procedure documentation
* Security compliance reports, such as PCI, ISO 27001, ISO 27002, SOC 2/3, SIG, CSA CSQ, etc.

​

1. GSA TTS will use these documents to assist in evaluating the organization’s security stance. As such, GSA TTS will give higher weight to those reports produced by independent auditors.

## 

#### Security of Data Including Personally Identifiable Information

* + - By acceptance of, or performance on, this contract, the Contractor agrees that in the event of any actual or suspected breach defined as loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to Personally Identifiable Information, whether physical or electronic)the Contractor must immediately (and in no event later than within one hour of discovery) report the breach to the GSA TTS Contracting Officer (CO) or the Contracting Officer’s Representative (COR) and the General Services Administration Incident Response Team. If the breach occurs outside of regular business hours and/or neither the CO nor the COR can be reached, Contractor must contact the POCs as specified by the CO or the COR for emergency contacts outside of business hours within one hour of discovery of the breach. Contractor must also notify the CO and COR and the General Services Administration Incident Response Team as soon as possible during regular business hours. Data breaches must follow reporting and response procedures as defined in GSA IT Security Procedural Guide 01-2, *Incident Response* and GSA Order CIO 9297.2C, *GSA Information Breach Notification Policy.*
    - Contractor states that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification to End consumers as a result of a breach must be coordinated with GSA TTS. The method and content of any notification by Contractor as a result of a breach will be subject to the approval of GSA TTS. In the event of a breach, Contractor assumes full responsibility for taking corrective action consistent with GSA Data Breach Notification Procedures (<http://www.gsa.gov/portal/directive/d0/content/675850>). Breach notifications involving PII are defined in section “Personally Identifiable Information Notification Requirement”.
    - Contractor also agrees to cooperate fully with the CO, the GSA Inspector General, and any other authorized Government investigator during any investigation regarding a breach or suspected breach of personally identifiable information. This cooperation includes providing access to documents and systems for a forensic investigation such as systems logs and server images, to determine how or why the breach occurred and how to prevent a similar occurrence in the future. Contractor must also correct, at its own cost, the system or protocol to prevent any future similar breach.

#### Personally Identifiable Information Notification Requirement

Subject to GSA analysis of the breach and the terms of its instructions to the Contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by GSA. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information. The Contractor agrees to assist in and comply with PII/Sensitive PII incident remediation and/or mitigation efforts and instructions, including those breaches that are not a result of the Contractor or employee actions, but the Contractor is an unintentional recipient of privacy data. Actions may include allowing GSA incident response personnel to have access to computing equipment or storage devices, complying with instructions to remove emails or files from local or network drives, mobile devices (BlackBerry, Smart Phone, iPad, USB thumb drives, etc...). In the event that a PII/Sensitive PII breach occurs as a result of the violation of a term of this contract by the Contractor or its employees, the Contractor must, as directed by the contracting officer and at no cost to GSA, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 24 months from discovery of the breach. Should GSA elect to provide and/or procure notification or identity protection services in response to a breach, the Contractor must be responsible for reimbursing GSA for those expenses. To ensure continuity with existing Government identity protection and credit monitoring efforts, the Contractor must use the identity protection service provider specified by GSA.