TRANSPORTATION SECURITY ADMINISTRATION (TSA)

Serial Number: TSA25-04-03472

Request for Information (RFI)

Requirements and Capabilities Analysis (RCA Office) Alternative Verification of Identity

---

I. INTRODUCTION

The Transportation Security Administration (TSA) has an emerging requirement for an alternative method of verification when a passenger cannot present an acceptable identity document. TSA is seeking a Contractor Owned and Contractor Operated solution to verify a passenger's identity in real time, without relying on the physical form of identification or their biometrics. TSA aims to have this technical solution provide a consent-based and scalable platform where the identity assurance services potentially are fee-based and funded by those who use the services.

The TSA is issuing this Request for Information (RFI) as part of its market research efforts, which is intended to improve TSA's understanding of market capabilities, identify qualified vendors, and finalize the acquisition strategy.

II. BACKGROUND

The mission of the Transportation Security Administration is to "Protect the nation's transportation systems to ensure freedom of movement for people and commerce." Prior to the COVID-19 National Emergency, TSA encountered over 2.5 million passengers a day and, on average, 600 instances of passengers without acceptable ID. These individuals are able to verify their identity via telephone through our National Transportation Vetting Center (NTVC). The agency is exploring other methods to verify an individual's identity that do not rely on physical identification or biometrics.

III. TECHNICAL SCOPE

TSA is seeking input from industry to provide a technical solution to confirm passengers' identities in close-to real time at the checkpoint without a physical form of identification. Vendors may have only the digital service application or the identity services requirements, although some vendors may have both services. Where a vendor can only meet one requirement set (i.e., digital application vs. identity assurance processes), the response should indicate ability to integrate with another vendor.

The objective is to use a digital services application to facilitate the verification of a passenger's identity at the checkpoint when they are not able to present a TSA-acceptable form of identification (available at

tsa.gov) to the TSA Checkpoint Officer. The digital services application will potentially be fee-based. In the event that a fee is collected, it would be for the purpose of offsetting the cost of operating the application and identity assurance services and would be paid directly to the application vendor. The TSA would not be party to the financial transaction nor be in receipt of any the funds generated by providing the service to the public.

The front end digital services application will allow passengers to enter limited biographic data elements and payment information that can securely liaise with back end databases of known entities.

Any solution will need to include a 2-step process:

1. A passenger's biographic data needs to be confirmed as both genuine, i.e., that it exists in a database(s), and is not fraudulent; and
2. The passenger claiming the biographic data is the same, i.e., not presenting another individual's or synthetic biographic data as their own.

The need for support is triggered by the following requirements:

1. Technical
    a. The system shall be able to process thousands of transactions per hour per day distributed across the TSA enterprise of airports;
    b. The potential need for the system to be able to receive and process payment directly from the passenger to fund application usage costs incurred by the vendor;
    c. The system shall be configurable with a front-end digital service application or website for passengers to use on their mobile phones;
        i. The app or website shall *not* derive the biographic data from a Machine-Readable Zone (MRZ) or Optical Character Recognition (OCR) scan of an identity document to enter the information;
        ii. The app or website shall have the capability to allow passengers to manually enter in their information;
        iii. The app or website shall not require a TSA provided network infrastructure;
        iv. The app or website shall have the capability to allow the end user (i.e., passenger) to review or ensure the entered biographic information is accurate; and
        v. The app or website must be compliant with section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) (codified at 29 U.S.C. § 794d).
    d. The front end digital service application or website shall be configurable to have passengers enter at least the following passenger biographic data elements:
        i. Name
        ii. Date of Birth (DOB)
        iii. Address, including street address 1 and 2, zip code, and state
        iv. Mobile phone number.
    e. The front end digital service application or website shall be able to interface with a back end database of known entities;
    f. The back end system shall have multiple unique sources for each element of identity information:

i. The system shall have different types of unique sources to include public, private, and regulated data;

g. The system shall be able to identify if the mobile phone has been or is being 'spoofed' or had its Subscriber Identification Module (SIM) card swapped;
h. The system shall be able to use a unique non-PII identifier to track and/or help create a configurable rule to potentially limit how many times a passenger can attempt to use this solution;
i. The system shall be able to provide an authentication/verification service to provide trust that the physical person owns the digitally verified biographic data, *i.e.*, the physical person is the same as the biographic data;
j. The system shall be capable of continuous (24x7) operation, with at least 99.9% monthly availability;
k. The system shall be able to generate both a human-readable and machine-readable result.
    i. The objective is to display to a Transportation Security Officer (TSO) that a passenger has a "pass" or a "fail" status
    ii. A machine-readable form factor should include the capability to be read by TSA's Credential Authentication Technology (CAT) machine, *e.g.,* a PDF 417 barcode or a Checksum format
        1. Data in the machine readable zone would include Name, DOB, and Gender to facilitate real-time Secure Flight screening

2. Identity Assurance

a. The system shall be able to reliably establish a person's identity and link it to a single, unique, and real-world identity;
b. The system shall be able to have configurable identity verification data modeling or algorithm(s) that best fit TSA needs and use cases;
c. The process shall use data modeling/algorithms to identify multiple risk indicators of stolen, synthetic, or otherwise fraudulent identities;
    i. Indicators may be associated with a collected identity attribute and/or linked from the third parties' database based on the collected attribute(s)
d. The process shall use the data elements to verify a known entity;
    i. A known entity can be verified if the Name, DOB, and Address exist (i.e., can be looked up) in the third parties' database
e. The process shall be able to "fuzzy" match to claimed name fields (i.e., Steve to Stephen, Suzanne Smith to Suzanne Alanna Smith to Suzanne A. Smith);
f. The process shall be able to match DOB by at least month and year of birth;
g. The process shall be able to match the claimed address to the most recent address in the third parties' database, including a match to the first 7 characters of the address;
    i. The process shall be able to determine if the claimed address is high risk, e.g., partially or entirely fabricated, or in an abandoned location
    ii. The process shall use data modeling/algorithms to identify inconsistencies with the history of a passenger's data that may indicate fraud;
h. The process of identity verification from the vendor should take less than 5 minutes to complete;

3. Privacy
    a. Third party applications shall comply with industry standards on credit card information storage and security;
    b. Third parties shall submit to TSA oversight on data protection/privacy guidelines and processes;
        i. Third parties must not use information collected during this process for any other purpose
    c. Third parties shall not store PII data on the front end digital services application;
    d. Third parties' platform(s) or information systems shall not interface within the boundaries of TSA's information systems.

IV. QUESTIONS FOR INDUSTRY

1. What is your company's depth of expertise with developing and maintaining the technical requirements listed above? Please provide a list of clients where this type of technical solution was used and provide a very brief project summary. If used at multiple clients, please focus your response on Federal Government clients.

2. What is your company's depth of expertise with developing and customizing identity assurance solutions meeting requirements listed above? Please provide a list of clients where this type of identity assurance solution was utilized and provide a very brief project summary. If used at multiple clients, please focus your response on Federal Government clients.

3. What is your company's depth of expertise with complying with the necessary privacy requirements listed above? Please provide a list of clients where your company complied with similar privacy requirements and provide a very brief project summary. If used at multiple clients, please focus your response on Federal Government clients.

4. Describe how your company implements identity assurance practices, including any applicable standards you adhere to.

5. Provide input or suggestions on the cost of a single identity assurance transaction.

6. Provide input or suggestions on ways to resolve the identity assurance problems at the checkpoint as a 'tier 1' solution with a complementary 'tier 2' solution in our National Transportation Vetting Center.
7. Which projects is your company actively working on with TSA? Does your company currently have teaming arrangements (partnerships/subcontracts) with firms performing the type of services detailed in the RFI?

8. Does your company currently have a DD-254 with the Federal Government? If so, what is the highest level sponsorship via Defense Security Service?

9. Provide input and recommendations on Key Personnel requirements, and what labor categories and skill sets your company typically proposes for similar services.

V. SUBMISSION OF INFORMATION

The information submitted in support of this RFI must be submitted in writing to the points of contact identified below. Responses must have a cover letter that includes the following information:

1. Company's Name
2. Company's Address
3. DUNS Number
4. Company's Size and Socio-Economic Status information
5. Technical Point of Contact(s) (Name, title, email, and phone number)
6. Contracting Point of Contact(s) (Name, title, email, and phone number)

The following sections provide a recommended outline for a response to this RFI. This outline is intended to minimize the effort of the respondent and structure the responses for ease of analysis by the Government.

Section 1- Corporate Expertise (1-2 pages)

Briefly describe the company, product and services, history, ownership, financial information, business size, and other information deemed relevant.

Section 2- Capabilities Statement (1-13 pages)

In order for TSA to improve it's understanding of market capabilities, provide a narrative description which identifies capabilities to meet the requirements identified in Section III/answer the questions in Section IV. The response can also describe what experience the company has providing similar and/or same services to other Federal Agencies.

Please follow the following response format:

- The TSA requests a written response to address any or all of the questions above. Responses should not exceed fifteen (15) pages in total. Written response shall be in either read-only Word or PDF format.
- Respondents should also include contact information should TSA have questions or want to hold further discussion.
    - Written responses shall be submitted no later than Friday, August 28, 2020 at 2:00pm Eastern Daylight Time to SRABriskintake@tsa.dhs.gov. Please contact SRABriskintake@tsa.dhs.gov via e-mail should you have any questions related to this RFI.
- Important Note: The vendor is not required to answer or comment on all content contained in this RFI in order to respond to this notice. Interested vendors are encouraged to share as many ideas and suggestions to all or some of the topics presented herein.

VI. REVIEW OF VENDOR RESPONSES

The Government will review vendor responses for market research purposes only. The Government does not intend to provide a response to submissions for this RFI, but the Government reserves the right to hold a technical information exchange meeting after the RFI review at the agency's discretion. Invitations to these meetings will be made available to those vendors from which TSA would like to obtain more information. These meetings will be scheduled at the discretion of the Government and may not be scheduled with all vendors that respond to the RFI. In addition to Government review, the TSA intends to have Deloitte, a support contractor, provide advisory services to review responses to this RFI. Therefore, it will be necessary to allow the aforementioned company to have access to all responses received from this RFI. As such, companies that intend to submit proprietary information to TSA and require a non-disclosure agreement to be executed between the TSA contractor and your company should notify Melyssa Bertucci via email.

VII. DISCLAIMER

This RFI is issued for information and planning purposes only and does not constitute a solicitation. All information received in response to this RFI that is marked *Proprietary* will be handled accordingly. The Government will not return or pay for any information provided in response to this announcement; no basis for a claim against the Government shall arise as a result from a response to this notice or Government use of any information provided. Responders are solely responsible for all expenses associated with responding to this announcement.