1. Statement of Work (Section J)

2. Purpose

The purpose of this Statement of Work (SOW) is to identify the tasks necessary to develop, deliver, and deploy private sector application capabilities expanding the public's enrollment opportunities for TSA Pre✓® through an Other Transactional Agreement (OTA) awarded by TSA.

TSA Pre✓®Scope:

TSA requests ready-to-market solutions to add private sector application capabilities for the TSA Pre✓® program to increase the public's enrollment access to the TSA Pre✓® program. As a secondary benefit, increasing enrollment access may lead to increasing scale for TSA Pre✓® and providing the ability for TSA to identify known travelers. Companies that want to propose a private sector application capability must demonstrate an ability to effectively market the TSA Pre✓® program to the flying public and successfully enroll and pre-screen a large population of applicants. This includes the ability to offer convenient and accessible enrollment options, reliably perform identity validation and verification as well as appropriately apply disqualifying criminal history convictions, and potentially make effective, provisional, determinations to pre-screen potential applicants for TSA Pre✓® eligibility.

3. Background

TSA Pre✓® is a voluntary program which allows low-risk travelers to be eligible for expedited screening at U.S. airports. TSA Pre✓® is an expedited screening program that allows pre-approved airline travelers to leave on their shoes, light outerwear and belt, keep their laptop in its case and their 3-1-1 compliant liquids/gels bag in a carry-on in select screening lanes. Travelers who choose not to enroll, or for some reason are not eligible, for TSA Pre✓® are not subject to any limitations on their travel and will instead, be processed through standard TSA screening before entering the controlled areas of airports. TSA also retains the authority to perform random screening on travelers who are authorized to receive TSA Pre✓® or other forms of physical screening.

The current TSA Pre✓® application program allows U.S. citizens, U.S. Nationals and lawful permanent residents to directly enroll in TSA Pre✓®. Once approved, travelers will receive a "Known Traveler Number" (KTN) and may be eligible for TSA Pre✓® lanes at select security checkpoints when flying on participating carriers.

Currently, there are several ways for individuals to enroll for TSA Pre✓®. These channels include the current Department of Homeland Security Trusted Traveler Programs, including TSA Pre✓® application program and the U.S. Customs and Border Protection (CBP) Global Entry, SENTRI and NEXUS programs. In addition, certain

other populations deemed to be low risk, such as certain Department of Defense personnel, are authorized to receive TSA Pre✓®.

In January 2013, TSA issued a Request for Information to conduct market research, technical demonstrations and testing of private sector capabilities to perform pre-screening of individuals for TSA Pre✓®. TSA requested that the respondents include the use of commercial, publicly available, and public records data (hereinafter collectively referred to as "commercial data") and algorithms to validate identity and perform low-risk determinations at an acceptable standard of performance at the selected risk threshold.

This initiative will expand enrollment into TSA Pre✓® by companies that receive Other Transactional Agreements (OTAs) from TSA. TSA's initiative with the companies awarded OTAs for the TSA Pre✓® program will allow these approved contractors to market, enroll and pre-screen individuals for TSA Pre✓® eligibility. TSA will make the final eligibility determination for actual TSA Pre✓® enrollment upon completion of TSA's threat assessment of an application that received successful pre-screened status and was forwarded by the pre-screening contractor.

TSA Pre✓® Expansion Approach:

Selected contractors shall receive an OTA from TSA to perform an initial, front-end pre-screening of applicants using proposed processes approved by TSA; of those applicants that qualify, TSA shall determine those applicants' eligibility for TSA Pre✓® through TSA's Security Threat Assessment (STA) process.

Contractors shall market TSA Pre✓® to potential applicants, in accordance with the TSA brand and approved licensing agreements, using their own industry partnerships and strategic business approaches, provide convenient and secure enrollment options and perform pre-screening of applicants to include identity validation, a criminal history records check and any additional approved, provisional, low-risk assessments.

Further high-level information about these processes is below with more detailed information contained in Section 4.

Eligibility Evaluation (Pre-Screening)

Contractors may use commercial data to conduct an eligibility evaluation (also known as pre-screening) of potential applicants. The eligibility evaluation shall include, at a minimum, validating identity and performing a criminal history records check to ensure that applicants do not have disqualifying convictions in conjunction with the TSA Pre✓® disqualifying offenses (please refer to the list of current disqualifiers available at http://www.tsa.gov/tsa-precheck/eligibility-requirements).

As a second component to the eligibility evaluation, TSA may also consider approving an option to use additional private sector processes to conduct a provisional risk assessment

(based on an algorithm developed by the Contractor) for the purposes of assisting in identifying those individuals believed to pose a low risk to transportation security. TSA must approve any commercial data inputs proposed for use by contractors to include those which validate identity and determine provisional low-risk status. If TSA determines that any particular commercial data inputs could potentially present disparate impacts to specific populations or is otherwise inappropriate, then TSA shall not approve those data inputs for use. Risk assessments may not be based on race, ethnicity, religion, national origin, age, financial status (e.g., credit ratings/scores, liens, bankruptcies, foreclosures, annual income), health records, constitutionally protected activity, or other records reflecting an individual's socio-economic status. Any algorithm used must receive DHS approval, which will be based upon a DHS evaluation requiring testing and review of commercial data inputs during that process.

Correction of Records (Redress) Based on Contractor's Eligibility Evaluation

Applicants who are found to be ineligible by the contractor and/or systems shall be notified by the respective contractor of the reason. Information about the available correction of records process, if relevant, and other available channels for TSA Pre✓® enrollment (such as, but not limited to, the TSA Pre✓® Application Program or U.S. Customs and Border Protection's Global Entry Program), including any alternatives available for identity assurance shall be provided in the notification. Contractors shall be responsible for offering a correction of records process to applicants for any determination of ineligibility related to any private sector pre-screening.

Submission of Applications to TSA

Contractors shall provide minimum required data elements (to include, but not be limited to, name, date of birth, gender, address, contact information, and country of birth, identity documents, and biometrics - at a minimum fingerprints) of the pre-screened applicants to TSA, via a secure interface TSA will determine final eligibility for TSA Pre✓®. Contractors shall not forward any information to TSA for applicants who are not successfully prescreened.

Fee Remittance

For each application submitted to TSA, Contractors shall transmit a standard fee, per applicant, in accordance with the Government's published fee notice, to TSA at the time of data transmission. As listed in the public fee notice, the fee will cover all of TSA's pertinent program costs, to include performing the STA. The Contractor shall act as TSA's agent to collect and remit fees in accordance with guidelines from applicable program regulations (such as 49 CFR 1572 for TWIC and HME programs) and from the TSA Office of Revenue and Department of Treasury. The Contractor shall daily remit fees electronically to TSA as fees are collected via TSA Office of Revenue approved methods such as the use of Treasury's online payment system, https://Pay.Gov form(s) and/or open collection interface (OCI).

The Contractor shall utilize all government banking services as TSA's agent representative of the government as part of the fee collection and fee submission process following processes and forms approved by TSA and US Treasury. The Contractor shall

coordinate with the TSA Office of Revenue and TSA program office for approval to establish Fee Collection and Remittance procedures.

Privacy Requirements

This OTA relates to the TSA Pre✓® Application Program System of Records. The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(a) The Contractor agrees to—

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies—

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this paragraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)

(1) “Operation of a system of records,” as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) “Record,” as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person’s name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) “System of records on individuals,” as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

4. Technical Requirements/Tasks/Outcomes

The Contractor shall provide enrollment services (including customer service) and applicant screening in support of expanding enrollment access by the general public to TSA Pre✓® benefit.

The sections below shall detail further the tasks required for the Contractor to (see also Attachment #1 - TSA Pre✓® Application Expansion High Level Requirements for further detailed requirements):

- Conduct Enrollment Activities
  - Online Pre-Enrollment Services
  - Identity Document Collection
  - In-Person Enrollment
  - Enrollment/Collection Personnel
  - In-Person Enrollment Location Logistics
- Conduct Identity Assurance Activities
- Conduct Eligibility Evaluation
  - Criminal History Records Check
  - Risk Assessment
  - Recurrent Vetting
- Transmit and Reconcile Application Data and Fees
  - Submit Applications to TSA
  - Fee Remittance
  - Receive Application Status Data from TSA
  - Notify TSA of Applicant Data Changes
- Provide Customer Service to Applicants
- Communications
- Enrollment Opportunities Marketing
- Data Storage and Usage
- Support Information System and Process Modifications resulting from TSA Legacy System Replacement or Enhancements
  - Usage of and integration with TSA Provided System(s)

- Retrieve Status from Enhanced or New TSA System(s)

4.1Conduct Enrollment Activities

The Contractor shall deliver and maintain the infrastructure and framework (including but not limited to personnel, facilities, hardware, and connectivity) necessary to support all aspects of the enrollment and registration process. The Contractor shall have the capability to collect, receive, store, and transmit applicant biographic and biometric (at a minimum fingerprints) information for application processing.

Applicants have the option to submit biographic information and identity documents online. However, all applicants shall be required to complete the in-person enrollment process with the Contractor for identity verification and biometric collection.

During both the optional pre-enrollment process and in-person enrollment, Contractor must present a TSA-approved privacy statement and obtain express authorization from the applicant for all uses of personally identifiable information (PII). Additionally, the Contractor shall notify the applicant that the name on the application must exactly match the name on the applicant's identity and proof of citizenship/immigration documents and be the name used when booking travel reservations.

Within 60 days of the start of testing activities outlined in Section 4.4 as well as receipt of Authority to Operate (as described in Section 4.14.3 – N), the Contractor shall begin accepting enrollments.

4.1.1 Online Pre-Enrollment Services

The Contractor shall establish a web-based pre-enrollment interface and process that shall allow applicants the opportunity to provide enrollment data online. The website shall allow the individual to enter biographical information and upload identity documents. A list of required data elements can be found in Attachment #2 – TPAE Technical Overview Document.

The web-based pre-enrollment should include error-checking routines to help eliminate common input errors and ensure completeness of the application.

Additionally, the Contractor shall have the flexibility to propose a telephonic pre-enrollment capability on top of the required applicant self-service web pre-enrollment capability.

Please note that while the Contractor is required to provide a pre-enrollment capability, applicants shall not be required to pre-enroll.

4.1.2 Identity Document Collection

The Contractor shall collect identity documents from the applicant using the TSA Pre✓® Application Program list of identity documents available at:
http://www.tsa.gov/tsa-precheck/required-documentation

Applicants may provide identity documents through one of the three options below:
1. Prior to the in-person enrollment process by uploading through the pre-enrollment website
2. During the in-person enrollment process
3. After the in-person enrollment process by uploading through the pre-enrollment website

Whether identity documents are uploaded prior to or after the in-person enrollment, the applicant must bring a government-issued photo ID to complete the in-person enrollment process.

The Contractor shall propose an approach for identity document authentication and a process for handling potentially fraudulent documents. The proposed approach and process shall be compliant with NIST 800-63 Assurance Level 3. (See Page 34 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf).

4.1.3 In-Person Enrollment

The Contractor shall provide enrollment services that include staffing and operations of in-person enrollment sites. The staff at the in-person enrollment site is referred to as "trusted agents".

Applicants have the option to provide biographical information and identity documents via a pre-enrollment website and appear in-person at Contractor enrollment sites to complete the enrollment process, or they may complete the entire enrollment process in-person.

Enrollment procedures at in-person enrollment centers may include but are not limited to any combination of identity verification, confirmation of application/enrollment data, submission of biometrics, and fee collection.

During the in-person enrollment process, the Contractor shall:

1) Capture required Personally-Identifiable Information (PII) and/or confirm PII entered during pre-enrollment.

2) Collect the required biometric data (at a minimum fingerprints compliant with the FBI's Electronic Biometric Transmission Specification version 10.0).

3) Verify the applicant's identity with the identity documents presented. Please note that while the applicant is required to provide identity documents to complete the application process, the documents may be uploaded in advance of the in-person enrollment process or after. At a minimum, the applicant must provide a government-issued photo ID to the in-person enrollment.

- If an applicant uploads documents in advance of the in-person enrollment process, the Contractor shall review the uploaded document(s) and verify identity during the in-person process.
- If an applicant uploads after the in-person enrollment process, then the Contractor shall review and validate the content of the identity documents before processing the application.

4.1.3.1 Biometrics Collection

The Contractor shall electronically collect fingerprints. Fingerprints captured must be compliant with the FBI's Electronic Biometric Transmission Specification version 10.0. Please reference https://www.fbibiospecs.org/ebts.html for details.

The Contractor shall propose various capture approaches (e.g., 2-print, 4-print, 10-print, etc.) and provide alternative options for individuals unable to provide fingerprints. TSA's preferred capture method is 10-print; however, any capture method proposed by the Contractor must be able to yield a verifiable match. Contractor procedures for fingerprint collection and transmission shall be provided to TSA for approval. The Contractor shall provide a rationale for the chosen biometrics capture approach, including performance metrics such as efficiency and effectiveness.

In addition to the fingerprint submission requirement, the Contractor may propose other biometric modalities for consideration of future capabilities by TSA. The Contractor shall describe the means in which the collected biometrics data will be transmitted to TSA.

4.1.3.2 Applicant Identity Verification

Currently, TSA accepts the following list of identity documents for the TSA Pre✓® Application Program:
http://www.tsa.gov/tsa-precheck/required-documentation

The Contractor shall propose to accept all or a subset of the TSA Pre✓® Application Program identity documents. Identity verification shall be compliant with NIST 800-63 Assurance Level 3. (See Page 34 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf).

While the applicant shall have the flexibility to upload documents before or after the in-person enrollment process, the applicant must present a government-issued photo ID during in-person enrollment.

If an applicant uploads documents before the in-person enrollment process, then when the applicant appears at in-person centers to complete the enrollment process, trusted agents shall confirm that the documents uploaded visually match the identity of the individual appearing at the enrollment center and that the documents are certified, unexpired and valid (as applicable to the document). If the applicant did not upload a government-issued photo ID, then the trusted agent shall capture the photo ID during in-person enrollment.

If an applicant presents identity documents during the in-person enrollment process, then the trusted agent shall confirm the documents presented match the identity of the applicant and capture the documents (if not done previously).

If the applicant does not have all necessary documentation during in-person enrollment (for example, if the applicant has a driver's license but forgot to bring their birth certificate), then the trusted agent will capture the photo ID only. The applicant shall be required to upload any outstanding identity document(s) before their application can proceed further. Once the outstanding identity document(s) have been uploaded, the Contractor shall validate and verify identity by comparing the information on the government-issued photo ID captured during in-person enrollment with the identity document(s) uploaded by the applicant. If any discrepancies exist between documents, the applicant shall be required to resolve the issues before their application can proceed further.

Please note that Identity Verification is a subset of the Identity Assurance Activities as described in **Section 4.2 – Conduct Identity Assurance Activities.**

4.1.4 Enrollment/Collection Personnel

The Contractor shall staff their locations with qualified and trained personnel, known as trusted agents. The Contractor shall be responsible to train their employees and ensure efficient background investigations and security training has been completed prior to hiring. Each employee shall be required to complete the TSA vetting process to include successful completion of a full STA (fingerprint based criminal history records check, citizenship, intelligence database check) and shall meet TSA Contractor Personnel Entry On Duty requirements (see Special Requirements and Management Directive 2800.71).

4.1.4.1 Personnel Training Plan

The Contractor shall provide a Personnel Training plan for TSA review and approval. The plan shall include both theoretical and practical (i.e. on the job) training. At a minimum, training must include annual TSA Information Security Awareness and Privacy training. The Personnel Training Plan shall detail the approach for initial, recurrent, and ongoing training.

4.1.5 In-Person Enrollment Location Logistics

The Contractor shall propose an approach to determining enrollment center locations for TSA review and approval. The Contractor shall set up enrollment locations in a way that shall protect applicant privacy and prevent inadvertent visual and aural disclosure of applicant information.

Physical security requirement for locations is required. Collection sites must meet physical security requirements as identified in Section 4.14 IT and System Security Requirements.

4.2 Conduct Identity Assurance Activities

In order to confirm the identity of an applicant to the program, the Contractor shall conduct identity assurance (i.e. to ensure that the applicant is who he/she is claiming to be).

In order to apply, individuals must provide Personally-Identifiable Information (PII) to the contractor as well as identity documents and fingerprints.

Please see **Section 4.1 -Conduct Enrollment Activities** for further details on the enrollment process. In-person identity verification is a required component of the identity assurance process.

The Contractor shall propose an identity assurance process, using the PII submitted by the applicant. For example, one option for identity assurance could include the use of Knowledge Based Authentication (KBA) quizzes.

After an applicant completes the in-person enrollment process, the Contractor may establish a "digital footprint" for the individual using commercial data to conduct identity assurance.

- This "digital footprint" must not use commercial data that unreasonably intrudes upon the personal privacy of an applicant. It may consider factors such as race, sex, age, and national origin only to verify the identity of the applicant. It should not rely on or evaluate factors such as religion, financial status, health records, constitutionally protected activity, or other records reflecting an individual's socio-economic status. The "digital footprint" may be used only for the purpose of generating identity assurance.

- The process shall validate the applicant's identity with a breadth of available public records which match the individual's information. The deeper and broader the digital footprint, the higher the confidence that the applicant's identity can be validated as known. Once a sufficient digital footprint has been developed, an additional layer of verification may be established to confirm identity. As mentioned previously, this additional layer of verification could include Knowledge Based Authentication (KBA) quizzes.

- Applicants will be permitted to take a KBA twice within 24 hours if there is a failure.

If the applicant is unable to successfully complete the identity assurance process, then the Contractor shall not submit the application to TSA and, instead, shall provide to the applicant other options to receive the TSA Pre✓® benefit (such as, but not limited to, the TSA Pre✓® Application Program or U.S. Customs and Border Protection's Global Entry Program).

As part of the test and evaluation/approval process, the Contractor shall be tested on a variety of identity/credentialing falsification or evasion techniques. Each Contractor

shall be tested on the same set of scenarios. Further tests will be conducted as part of continuous evaluation to ensure that previously undiscovered vulnerabilities are closed as various falsification, evasion, or spoofing techniques evolve.

4.3 Conduct Eligibility Evaluation

The Contractor shall also use the PII submitted by the applicant to perform an eligibility evaluation, which may consist of two components:

1) Criminal history records check (CHRC)
2) Risk assessment (only if using a process/algorithm approved by DHS)

4.3.1 Criminal History Records Check

After the identity assurance process has been successfully completed, the Contractor shall search commercial data for evidence of convictions for disqualifying crimes. The Contractor shall describe all data sources utilized to determine that all criminal history associated with an applicant has been evaluated.

The Contractor shall perform a criminal history records check against Parts A and B of the disqualifying offenses currently used for the TSA Pre✓® Application Program available at: http://www.tsa.gov/tsa-precheck/eligibility-requirements

The Contractor shall have the ability to automatically disqualify applicants based on the current TSA Pre✓® disqualification list and the ability to comprehensively find and evaluate all pertinent information necessary to achieve an acceptable standard of performance at the selected risk threshold that all criminal history associated with an applicant has been evaluated. Per the TSA Parts A and B of the current disqualifying offenses, this includes Permanent Disqualifying Criminal Offenses, in which a person is disqualified if he or she was convicted or found not guilty by reason of insanity for any of the felonies listed, and Interim Disqualifying Criminal Offenses, in which a person is disqualified if he or she was convicted or found not guilty by reason of insanity within the previous seven years or was released from prison in the last five years for any of the felonies listed.

The Contractor shall notify the applicant of their ineligibility and how to apply for redress in the event a disqualifying crime is found. It will be incumbent upon the applicant to obtain corrected records for reconsideration by the Contractor. If corrected records are successfully presented by the applicant, then the Contractor shall continue processing of the application.

4.3.2 Risk Assessment

If directed by DHS to turn on risk assessment functionality, the Contractor shall use their DHS-validated algorithms to perform a provisional risk assessment. This capability may or may not be turned on at initial deployment as directed by TSA. A contractor's algorithms may be automated platforms. If the capability is turned on, then the algorithms shall be scalable and flexible to adapt to changing risk environments, and government requirements, including removing datasets the government determines

should not be utilized due to the protection of privacy and civil liberties guarantees. Algorithms may use commercial data as weighted inputs to develop a score.

Commercial data elements and risk algorithm must undergo DHS review prior to use. **Within 10 days of contract award, the Contractor shall be ready to begin DHS testing of the risk algorithm and successfully complete testing within 60 days of testing start.**

Commercial data risk algorithm categories may not include, and risk assessments may not be based on race, ethnicity, religion, national origin, age, or financial status (e.g. credit ratings/scores, liens, bankruptcies, foreclosures, annual income), health records, constitutionally protected activity, or other records reflecting an individual's socio-economic status), and must not unreasonably intrude upon personal privacy. A score under the threshold indicates that the applicant can be identified as a low risk to transportation security. TSA will provide guidance on acceptable risk and contractors will select a threshold at or above that level based on their own risk tolerance. Contractors shall not apply the risk assessment score or any determinations made under it for any purposes other than the TSA Pre✓® Application Expansion eligibility evaluation.

TSA shall require continuous improvement of any approved private sector solutions and a review process will be in place after OTA award whereby TSA must approve any changes to algorithms, to include the addition or deletion of any data inputs, as well as any other system upgrades and review formulas. In order to approve changes to commercial data inputs, TSA may perform additional tests to determine the analytics capability of the algorithm as well as any potential disparate impacts to specific populations or unreasonable privacy intrusions. It is expected that continuous improvement may also help Contractors improve both their security performance and enrollment rates over the life of the agreement with TSA by allowing Contractors to work with continuously expanding and improving training data elements. Government personnel shall have unlimited access to commercial data and software/code.

If use of the risk assessment has been directed by TSA (the capability may not be turned on if not approved by DHS), then:

- If the applicant is unable to pass the risk assessment, then the Contractor shall notify the applicant of their ineligibility and how to apply for redress. It will be incumbent upon the applicant to obtain corrected records for reconsideration by the Contractor. If corrected records are successfully presented by the applicant, then the Contractor shall continue processing of the application.
- However, if the applicant is unable to pass the risk assessment and cannot provide corrected records, then the Contractor shall not submit the application to TSA and, instead, shall identify other options to receive the TSA Pre✓® benefit (such as, but not limited to, the TSA Pre✓® Application Program or U.S. Customs and Border Protection's Global Entry Program).

TSA and DHS may instruct the Contractor to turn off the risk assessment capability at any time.

4.3.3 Recurrent Vetting

The Contractor shall be capable of conducting recurrent eligibility evaluations and propose a recurrent applicant vetting strategy. This capability may or may not be turned on at initial deployment as directed by TSA.

The Contractor shall make redress available to applicants with potentially disqualifying information as described in Sections 4.3.1 and 4.3.2.

4.4 Transmit and Reconcile Application Data and Fees

The Contractor shall integrate with TSA and US Treasury systems. Specific integration requirements are detailed below.

Within 45 days of contract award, the Contractor shall be able to begin integration/interface testing (to include TSA and pay.gov testing).

Furthermore, within 60 days of the start of testing, the Contractor shall complete end-to-end and volume testing with all TSA and TSA-required systems to include TSA and pay.gov.

4.4.1 Submit Applications to TSA

In order for an application to proceed for a TSA security threat assessment, the applicant must have:

1) Successfully completed the identity assurance process (as described in **Section 4.2**)
AND
2) Passed the eligibility evaluation (as described in **Section 4.3**)

If the applicant meets the above criteria, then the Contractor shall generate a unique KTN, based on a numbering configuration provided by TSA, for that applicant.

The Contractor shall transmit the applicant's biographic data, biometric data, identity documents, and unique KTN to TSA in accordance with the technical overview document provided as Attachment #2 – TPAE Technical Overview Document. The Contractor shall have the capability to receive and record/track acknowledgement of receipt of transmission from TSA. Furthermore, the Contractor shall have the capability to retransmit application data as necessary to resolve transmission issues that may arise.

4.4.2 Fee Remittance

The Contractor shall collect and remit payment to TSA, pursuant to 6 U.S.C. 469, for each application that they submit. The Contractor shall remit fees to TSA in form and manner consistent with Attachment #3 - Fee Collection Requirements, describing requirements for the collection of government funds.

The information provided in Attachment #3 was obtained from the website of Treasury's Financial Management Service (FMS). These materials are subject to change, and throughout the duration of the contract, the Contractor will be required to comply with the

provisions of whichever version is then in effect. For the most current version of the materials, please refer to FMS's website at www.fms.treas.gov. The Treasury Financial Manual (TFM) can be found in the "FMS Publications" section, under the heading "Regulations and Guidance." All of the TFM materials in Attachment #3 can be found in Volume I of the TFM. Pay.gov materials, including the FMS credit card processing rules, can be found in the "FMS Programs" section, under the heading "Collections."

The Contractor shall remit payment/fees to TSA as applicable to the program prior to transmitting the enrollment/application to TSA. TSA will not issue fee refunds once vetting services have commenced. The Contractor shall remit fees to TSA via automated clearing house (ACH) direct debit through Pay.gov Trusted Collection Services (TCS). TCS requirements are outlined in Attachment #3. Additionally, technical TCS requirements to achieve interface with US Treasury and TSA will be available from the TSA Contracting Officer upon vendor selection. The Contractor is not authorized to remit cash to TSA. The Contractor is responsible to establish procedures for the submission of the fee and provide to TSA for approval. Transmission of program fees to TSA must be compliant with US Treasury requirements including DAILY transmission of TSA fees as they are required and include payment confirmation by the government at the application/individual/transaction level.

The Contractor shall provide the ability for bulk payments (for example, an employer or sponsor may choose to pay for the fees for all its employees).

The Contractor shall remit TSA fees in accordance with program fee requirements and regulations and have the flexibility to adjust fee remittance procedures and amounts remitted if legislation, regulations, policies or requirements change.

4.4.2.1 Fee Reconciliation

The Contractor shall establish a financial collection and reconciliation process including collection and reconciliation report(s). The reconciliation shall track applications against remittance made to the Government. When transmitting remittance made to the Government, the Contractor shall provide a report detailing the remittance submitted against the number of applications and the number of applicants processed.

The Contractor shall establish a Financial Collection and Reconciliation process which shall include a report that shall provide the following information but not be limited to:

- Track enrollment applications with remittance (in summary as well as individually in detail)
- Match identity and enrollment center (when applicable) and remittance
- Establish a process to reconcile any errors, report the errors and progress of the resolution

4.4.3 Receive Application Status Data from TSA

Upon receipt of a complete enrollment package and the corresponding fee, TSA will initiate the STA. The TSA STA shall include checks against government databases and watchlists associated with security and immigration to determine eligibility. TSA shall

make the final determination on acceptance or denial into TSA Pre✓ ® and notify the applicant of their eligibility or ineligibility and any available TSA redress procedures. Applicants should expect to receive notification from TSA in 2-3 weeks.

TSA shall provide status of the approval process *(e.g. in-process or complete)* to the Contractor for customer service purposes. For approved applicants, TSA shall notify the applicant and inform them of their KTN.

TSA shall communicate application status in accordance with the technical overview document provided as Attachment #2 – TPAE Technical Overview Document.

4.4.4 Notify TSA of Applicant Data Changes

For applications that are sent forward to TSA for processing, the Contractor shall notify TSA when applicant information changes.

Changes could include, but are not limited to:

- KTNs that are no longer valid (for example, in the case of revocation due to disqualification or expiration of the associated benefit that the applicant has with the Contractor)
- Contact information (mailing address, phone number, email address)
- Data corrections (could include, but are not limited to, name, date of birth, country of citizenship, country of birth, etc.)

These changes shall be communicated to TSA in accordance with the document provided as Attachment #2 – TPAE Technical Overview Document.

4.5 Provide Customer Service to Applicants

The Contractor shall propose a customer service strategy to support applicants whom they enrolled, to include customer service availability. Applicants could either contact the Contractor directly or be referred to the Contractor by TSA.

Options for customer service include, but are not limited to, one or more of the following capabilities:

- Website
- Telephonic support via a call center
- E-mail support

In the customer service strategy proposal, the Contractor shall include their proposed Acceptable Quality Levels (AQLs) for each capability.

Please reference **Section 4.10.1 – General Performance Metrics** for TSA's minimum Customer Service predefined AQLs.

Customer service capabilities should account for the following types of questions (this list is not comprehensive):

- In-person enrollment locations

- Program eligibility requirements
- Application status questions
- Correspondence sent by the Contractor
- Contractor's redress process
- Correspondence sent by TSA
- Applicant contact information updates (contact method, phone number, email address, mailing address)
- Data corrections (such as, but not limited to, name, date of birth, etc.)

4.6 Applicant Communications

The Contractor shall propose an applicant communications approach. This approach should account for the following items (this list is not comprehensive):

- Deployment of in-person enrollment locations
- Mobile enrollment activities and opportunities
- Messaging to applicants when enrollment sites are closed temporarily, permanently, and/or changing location.
- Messaging to applicants regarding enrollment site hours of operation, directions, etc.
- Messaging to applicants regarding system or operational issues impacting enrollments
- Messaging to applicants regarding policy changes (ex. acceptable enrollment documents)

4.7 Enrollment Opportunities Marketing

The Contractor shall provide a marketing approach that illustrates how the Contractor plans to offer application opportunities for enrollment into the TSA Pre✓® program. The Contractor shall detail any plan to employ strategic business approaches such as affinity marketing partnerships, etc., and clearly articulate how its marketing efforts and communications align with established TSA Pre✓® brand identity and positioning, including consistency in tone and language. The Contractor must execute a TSA-approved licensing agreement to abide by all specified TSA Pre✓® branding strategy guidelines. Please reference Attachment #4 – TSA PreCheck License for OTA, Attachment #5 - TSA Brand Positioning, and Attachment #6 – TSA Branding Guidelines.

Consistent with the TSA Pre✓® branding strategy guidelines and TSA Licensing Agreement, a Contractor's marketing approach must:

- Coincide with TSA Pre✓® brand strategy and positioning to include consistency in tone and language, including with respect to protecting privacy and civil liberties.
- Obtain TSA concurrence within 30 days of contract award to ensure consistency in messaging and overall communications
- Identify partnership marketing agreements already in place with contractor's own vendors for effective market outreach on TSA Pre✓® application

- Demonstrate verifiable agreements with travel industry providers (airlines, travel agents, corporate travel departments, hotels, etc) that outline commitment to identify, message and encourage the general travelling public's application to enroll in TSA Pre✓®.
- Agreement not to assert TSA position or approval relating to Contractor's communications. Contractor marketing communications may not commit or appear to commit through implied association a deliverable or attribute that is not specifically approved for publication by TSA. For example, TSA will not mention or make wait-time claims relating to TSA Pre✓® or Standard Lanes within TSA communications, thus contractor marketing materials must not make such a claim.
- Pricing/Business Model for the Public Enrollment Fee.

The Contractor shall market its opportunities for TSA Pre✓® applications and prescreening capabilities in accordance with a TSA Pre✓® branding strategy guidelines Contractor will represent itself as an independent entity, and not as an affiliate of the TSA or DHS. Any use of the TSA Pre✓® trademark on Contractor Materials shall include the following or similar credit, as appropriate: ***"Contractor is not a government entity or affiliated with the Federal government. Contractor provides pre-enrollment services for the Transportation Security Administration's TSA Pre✓® Risk Based Screening program. The TSA Pre✓® trademark is used under license with the permission of the U.S. Department of Homeland Security."*** The notice must be displayed in a type font of legible size.

The TSA Pre✓® trademark constitutes DHS-owned intellectual property, and is used in connection with the Department's efforts to facilitate expedited security screening experiences for selected travelers of participating airlines. With its execution of the approved licensing agreement, DHS confers to Contractor a nonexclusive, nontransferable, royalty free use of the TSA Pre✓® trademark, including the right to copy, display and distribute, for the sole and exclusive purpose of including the trademark on materials authorized by DHS as part of contractors marketing to prospective TSA Pre✓® Program members.

To maintain the legal protections associated with the trademark, TSA on behalf of DHS must control the use of the trademark. The Contractor agrees that no modifications to DHS-provided Materials will be published without TSA review and prior written approval from TSA (email communication is sufficient) other than the inclusion of "Contractor's" logos and other necessary data. Contractor also agrees that it shall not use the trademark in a manner or context that reflects unfavorably upon any component of DHS or which will diminish or damage the goodwill associated with the TSA Pre✓® trademark.

Accordingly, the Contractor's marketing materials must be "non-controversial," meaning the advertisements will be consistent with normal standards for mainstream public advertising, as well as DHS and TSA media policy. In addition, the term precludes any political advertising, including but not limited to those pertaining to candidates, issues,

parties, campaign committees, specific elections, etc., or any other advertising that may create a sense of sponsorship or imply endorsement by the government. Additionally, to protect and ensure the Governments interest against dilution of the TSA Pre✓® trademark, i.e., dilution by "blurring" and/or dilution by "tarnishment", for Materials created by Contractor regarding participation in the TSA Pre✓® Program, Contractor agrees to release the Materials only after obtaining TSA's prior written approval (email communication is sufficient). TSA prior approval is not needed for each individual item, provided that the use is substantially the same as prior approved materials. TSA will provide approval for classes of items associated with advertising.

4.8 Data Storage and Usage

All applicant data collected and stored by the Contractor for the purpose of applying for TSA Pre✓® must be held in a separate database that can follow TSA prescribed data retention requirements.

The Contractor shall not use data collected from applicants for any purpose other than pre-screening for TSA Pre✓®unless the Contractor obtains express permission from the applicants after completion of the enrollment process for the program.

The Contractor must clearly distinguish the completion of the enrollment process for TSA Pre✓® before requesting permission from applicants to continue communication regarding any other marketing opportunities not affiliated with TSA Pre✓®. Any such marketing communications would require the applicants to affirmatively opt-in to such additional marketing.

Contractors are prohibited from using, in any capacity, information pertaining to an applicant's risk including the interim and final determinations for TSA Pre✓®. All prohibitions must be clearly stated in Terms and Conditions which are presented to applicants at the beginning of the enrollment process prior to the collection of information.

4.9 Support Information System and Process Modifications resulting from TSA Legacy System Replacement or Enhancements

Initially, the Contractor will integrate with TSA's legacy system known as the Consolidated Screening Gateway (CSG) system. However, the Contractor shall demonstrate and have the capability to make changes to its information management systems and service procedures resulting from enhancements to the legacy system, or due to the planned future replacement of TSA legacy systems.

TSA Legacy System Enhancements: The Contractor shall develop a flexible and configurable system and enrollment services structure (including resourcing and processes) to facilitate changes and enhancements made to TSA legacy systems, processes and external interfaces at the Contractor's expense.

TSA Technology Modernization: Changes shall be required to update information management systems resulting from the replacement of TSA legacy systems with a new, modernized system and processes.
The Contractor's interface will eventually need to be rebuilt from the legacy CSG system to the TSA Infrastructure Modernization (TIM) system at the Contractor's expense.

4.10 Performance Metrics

The OTA Contractor shall provide services within the Service Level Agreements (SLAs) defined below. The SLAs have been established to evaluate OTA Contractor performance. These metrics may also provide a benchmark to identify areas for future improvements.

The OTA Contractor shall, to the maximum extent possible, meet or exceed the desired outcomes summarized in the tables below. These objectives are of equal importance to the Government. Acceptable quality levels (AQLs) are defined as the minimum level of performance accepted by the Government. The OTA Contractor shall support each performance measure with statistically valid data collection processes detailed in the Contractor's QCP.

If the OTA Contractor does not meet the AQLs or performance measures as defined in sections 4.10.1 and 4.10.2 below, then TSA may terminate the OTA per article xxx.

Comment [LT1]: Gloria – please fill in

4.10.1 General Performance Metrics

Number.	Performance Measure	Definition	Desired Outcome/ Acceptable Quality Level (AQL)	Reporting Frequency
	Quantifiable, outcome-focused indicators used to evaluate the degree of success achieving the statement of work's objectives (e.g. help desk response time, fingerprint rejection	***The specific definition for a performance measure, to include description and intent.***	***The minimum level of performance accepted by the Government***	***How often the metric should be reported to the Government***
1.	Technical – *SLAs to be achieved immediately upon 1st enrollment.*			

	a) System Availability	System availability is defined as being available 24X7 and providing correct and up-to-date information for the applicants with no erroneous information. *System availability includes all system functions (in-person enrollment, web enrollment, data transmission to TSA or TSA specified systems) System availability is exclusive of planned system maintenance downtime.*	A minimum 99% availability in a given measurement period (one month) is expected.	Monthly
	b) Application/Enrollment Rejection Rate	The percentage of applications/ enrollments rejected by the TSA or TSA authorized receiving system (such as the Consolidated Screening Gateway) due to mismatched, , incorrectly formatted or incomplete application data.	≤ 0.5% of submitted applications/enrollments	Monthly
	c) Data Correction Rate	The percentage of applications/ enrollments requiring data correction by the Contractor due to incorrectly entered data (such as, but not limited to, typographical errors in the name or date of birth)	≤ 0.5% of submitted applications/enrollments	Monthly
2.	Security– *SLAs to be achieved immediately upon 1st enrollment*			

	a) Security Violations	A security violation is defined as a compromise or suspected compromise of information to persons not authorized to receive that information, or a serious failure to comply with the provisions of applicable security requirements which is likely to result in compromise. A practice dangerous to security is defined as any knowing, willful, or negligent action contrary to the provisions of applicable security requirements that does not rise to the level of a security violation. A pattern of repeated lesser security infractions committed by Contractor personnel may result in determination of a practice dangerous to security.	0 violations The Contractor does not commit any security violations or engage in any practices dangerous to security. The final determination as to the classification and severity of a security incident as either a security violation or practice dangerous to security is at the discretion of the responsible TSA Security Officer(s) and TSA Management Official(s).	As soon as the violation is discovered
3.	Privacy – *SLAs to be achieved immediately upon 1st enrollment*			

	a) Privacy breach	A privacy breach is defined as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.	0 breaches The Contractor does not commit any privacy breach. The final determination as to the classification, severity, and remedy of a privacy breach is at the discretion of the responsible TSA Security Officer(s) and TSA Management Official(s).	As soon as the privacy incident is discovered
4.	Customer Service –*Call Center SLAs (a-d) to be achieved within 60 days of Call Center opening.*			
	a) Operational Availability	The percentage of time that an enrollment center is open (number of hours closed/ number of scheduled operational hours)	99%	Monthly
	b) Call Center *and Technical Help Desk* Telephone Response Time	Time on hold once connected *to the telephone line*	1.5 minutes	Monthly

	c) Call Center Resolution Time	Average time to resolve inquiries (excluding phone enrollments) made by applicants	7 minutes	Monthly
	d) Speed to Answer	Percent of calls to the customer enrollment center and help desk answered *(either via IVR or person)* within a specific period of time	80% of calls answered within 10 seconds	Monthly
	e) Call abandonment rate	Percentage of calls that are abandoned before the caller speaks to a Help Desk Operator/Customer	≤ 5% of calls	Monthly
	f) Response time to email inquiries	Average time to satisfactorily answer questions sent by email	< 3 business days	Monthly

Critical Customer Service Measures are further defined below:

Operational Availability – This is defined as the percentage of time that an enrollment center is open in relation to its scheduled hours.

# of hours open

# of scheduled hours

1. Any closures related to weather shall not be included in this metric.
2. Federal government holidays (for example, Veterans Day) shall not be included as part of scheduled hours since it is anticipated that all enrollment centers shall be closed during these holidays.

4.10.2 Identity Assurance and Eligibility Evaluation SLAs

The following minimum requirements are applicable for all algorithms proposed and must be met for contractors to be eligible to enroll passengers for TSA Pre✓®. In addition, similar criteria will be used to re-validate any algorithms that might be used on an annual basis following audit and compliance testing. Security related benchmarks and evaluation criteria are SSI and will be discussed with awarded Contractors during testing and evaluation (T&E) and approval. Requirement Categories include the following:

Identity Assurance	**Risk Categorization and Scoring Reconciliation**	**General Algorithm Configuration and Reporting**
All criteria metrics related to verifying and reconciling the identity of an applicant, prior to running a criminal history records check and a risk assessment algorithm.	All criteria metrics related to the decision making process and technical approach for assigning risk scores to individuals.	All criteria metrics related to the algorithm's ability to adapt, improve, and perform under specific parameters.

Requirement Category	Title	Definition	Rationale	Measure of Success
1. Identity Assurance	Identity Verification Specification	Contractors shall describe the following: -Identity verification process *(credentials, digital footprints etc.)* -*Commercial data inputs* -Identity confidence score scale *(e.g. Irreconcilable, High Risk , Low Risk)* -Identity confidence scoring inputs, methodology and logic -Relevant third party consortium members -Validation and quality control protocols -Alternate identity verification processes -In-person ID	The quality of the identity verification process for use in the algorithm provides confidence in determining if the identity is successfully resolvable to an individual applicant. Increasing identity data *(i.e. better address information*) should decrease the number of unresolvable identities, resulting in less applicants filtered out before the risk scoring is analyzed.	A consistent, understandable, and defensible identity verification process with an associated identity confidence score for all applicants.

		verification airport application concept of operations (CONOPS) which includes but is not limited to: a) The ID authentication procedure and needed equipment and materials along with estimates of processing time per passenger, and b) The time required to verify identification on a per traveler basis at the airport in an operational environment -Beyond the proscribed use of fingerprints, describe the ID verification methodology, including but not limited to: a) and additional biometric methods, b) and non-biometric methods, c) combinations of biometric and non-biometric methods, and d) which methods will be implemented in real-time at airports and which ones will occur prior to passenger air travel either online or in person at a verification facility		
2. Identity Assurance	Identity Confidence Scores	Contractors shall provide the following: -Identity confidence score for each applicant *(i.e., how confident is the algorithm that applicant identity has been established at time of enrollment)* -Provide an Identity Confidence Distribution, along with accompanying qualitative and/or quantitative rationale and any relevant quantitative and	Classifying an applicant as high or low risk will be affected by the quality of data output from the initial identity verification step. The identity confidence score is an indicator of the quality of the data going into the algorithm. Identity confidence is important in testing given legal/privacy restrictions that limit the use of SSNs, which could be utilized in live operations.	100% of applicants have an identity confidence score that is computationally sound and defensible.

		qualitative analysis for the Identity Confidence Histogram/Distribution	Identity Confidence Distribution information requirements will enable better understanding of how "confidence" is scored.	
3. Identity Assurance	Identity Confidence Threshold	Contractors shall describe the following: -Identity Confidence Score Threshold (T_{ID}) used to classify an applicant as requiring additional identity verification *(irreconcilable identity)* or as eligible for algorithm risk scoring *(e.g., at what point can contractors not establish identity and how is that determination made?)* -A qualitative and quantitative rationale for the Identitfy Confidence score Threshold (T_{ID}) chosen	The government needs to understand, from the algorithm results, how many records were deemed irreconcilable and could not be used in the algorithm. Contractors should provide enough detail for the agency to understand how IDs were binned as irreconcilable IDs versus those able to be processed in the algorithm.	100% of applicants with Identity Confidence Scores < T_{ID} are classified as -1 *(irreconcilable identity).* 100% of applicants with Identity Confidence Scores >= T_{ID} are classified as 0 or 1 *(high/low risk).*
4. Identity Assurance	Identity Verification Acceptance Rate	Contractors shall demonstrate the following: -Identity acceptance rate in testing *(e.g., how many identities for applications can be positively identified and pass through to screening process?)* -Describe how ID verification vulnerability exploits will be resolved in a timely manner and how patches will be implemented at a national level	A large percentage of the traveling public is considered low risk, with an acceptable confidence score in their identity resolution. Contractors must have the ability to identify an acceptable confidence score for an identity to be reconciled and considered resolved.	100% of applicants with verifiable identities are processed by the algorithm for risk scoring.
5. Criminal History Records Check	Minimum Criminal Disqualifiers	The contractor shall demonstrate: The ability to automatically disqualify	<u>Permanent Disqualifying Criminal Offenses</u>: A person will be disqualified if he or she	100% of applicants are checked against government minimum KTN

		applicants based on the current TSA Pre✓® disqualification list The ability to comprehensively find and evaluate all pertinent information necessary to achieve an acceptable standard of performance at the selected threshold that all criminal history associated with an applicant has been evaluated.	was convicted or found not guilty by reason of insanity for any of the felonies listed. <u>Interim Disqualifying Criminal Offenses</u>: A person will be disqualified if he or she was convicted or found not guilty by reason of insanity within the previous seven years or was released from prison in the last five years for any of the felonies listed.	disqualifiers; use of open source and address enriched biographical data.
6. Risk Categorization and Scoring Reconciliation	Risk Score Algorithm Specification	Contractors shall describe the following: -Structural decision-making process and technical machine learning approach. -Algorithm training and feature/data input selection process. -Algorithm data elements/inputs. Contractors shall provide the following: -Executable code to independently test authority -Itemization of additional manual and/or quality control steps -Risk score scale (0 = lowest risk) -Algorithm validation and quality control -The current state of the algorithm by providing a definition for each factor and a description of how that factor contributes to algorithm	The contractor shall provide sufficient detail for DHS/TSA to understand the steps, technologies, and/or mathematical techniques used for risk score determination in the algorithm. The contractor shall provide the data attributes that provide an ordered list of data attributes based on their impact on the overall score. The private sector entity shall be able to provide relevant attribute numbers/scores to describe the sensitivity of the algorithm; whatever selected attributes satisfy each decision criteria. “Sandbox” versions of the Contractor’s algorithm are for verification and validations purposes Data quality control plan requirements captures how existing	A consistent, understandable, and defensible machine learning algorithm with an associated risk score for all applicants whose identity has been verified.

		outputs including qualitative and quantitative criteria for "high risk" and "low risk" determinations. This information will be treated as PCII by the Federal Government. -A description of all data sets they plan to use for passenger risk evaluation -In year 2 of the OTA, the Contractor shall provide a version of the algorithm that shall be structured to allow execution with text-based data feature inputs independent of any commercial database or criminal records base. This will allow inclusion in a "sandbox" type testing and evaluation (T&E) arena at TSA. This algorithm shall be a "sandbox" version of its algorithm which can be used in stand-alone tests with simulated data, without linking to online databases, for T&E and for audit and compliance purposes -A data quality control plan to ensure the integrity and the reliability of the data they utilize (whether Contractor-owned or 3rd party) and shall include the following elements: where does the data come from, how it is gathered, patterns of any data anomalies (e.g. deceased individuals, missing data elements), how often are the data sources updated, if records are obtained	data elements evolve over time and how that evolution impacts algorithm performance.	

		from an outside source, what quality control processes does this source use, which groups of people are omitted from this database (e.g. college students, geographic locations) -The Contractor shall work with the Government to test efficacy if the Contractor plans to change the algorithm		
7. Risk Categorization and Scoring Reconciliation	Risk Scores	The contractor shall provide the following: Risk score for each applicant whose identity has been verified *(If the contractor uses a scaled risk score, how are applicants performing across risk scores?)* The algorithm shall include not only the high risk and low risk classifications but the ability to produce statistics on any of the demographics used in the algorithm as they relate to high risk and low risk determinations	The screening process, using the private sector algorithms, requires scoring each applicant to a high level of risk *(for denial of a Known Traveler Number)* or scoring to a low level of risk *(for acceptance of a Known Traveler Number).*	100% of identity verified applicants have a risk score that is computationally sound and defensible.
8. Risk Categorization and Scoring Reconciliation	Risk Score Threshold	The contractor shall provide the following: Risk Score Threshold (T_{RS}) used for high/low risk classification (At what point on a risk score does an applicant receive/not receive a KTN?) A qualitative and quantitative rationale for the Risk Score Threshold (T_{RS}) chosen for high/low risk classification	Contractors should provide enough detail to explain how each individual record was classified as high or low risk after being processed in the algorithm.	100% of identity verified KTN determinations have an associated Risk Threshold (T_{RS}) value. 100% of identity verified applicants with risk scores $< (T_{RS})$ are classified as 1 *(low risk).*

		Any algorithm in use has an adjustable risk threshold		100% of applicants with Risk Scores >= (T_{RS}) are classified as 0 *(high risk).*
9. Risk Categorization and Scoring Reconciliation	Low Risk Enrollment Rate	The contractor shall demonstrate the following: Suitable low risk enrollment rates in testing (test sensitivity). Fraction of low risk applicants and verified identities recommended for Known Traveler Number (KTN) issuance. Fraction of all low risk applicants recommended for KTN issuance. Algorithm evaluation shall be based on an Area-Under-the-Curve (AUC) metric and other signal processing theory metrics. The Contractor solution shall have an objective to identify bad actors in government provided test-sets with an effectiveness greater than a government determined benchmark (which will be treated as SSI) while simultaneously achieving a maximum of a 50% false negative rate (deny KTN to non-risky persons). At a minimum, evaluations will utilize the following metrics: AUC for a ROC curve, false negatives for a given benchmark on the ROC curve, % of known bad actors from government-provided test-sets excluded from	A large percentage of the traveling public is considered low risk and could be issued a KTN by the private sector entity. The contractor should have the ability to correctly identify low risk travelers for enrollment based on a risk score that can be assigned comparable to a baseline threshold.	<u>Objective</u>: 100% of low risk applicants with verified identities are classified as low risk 100% of all low risk applicants are classified as low risk <u>Minimum Threshold</u>: x% of low risk applicants are classified as low risk y% of all low risk applicants are classified as low risk

		receiving a KTN, % of known good actors from government-provided test-sets excluded from receiving a KTN		
10. Risk Categorization and Scoring Reconciliation	High Risk Exclusion Rate	The contractor shall demonstrate the following: Suitable high risk exclusion rates in testing *(test specificity)*. Fraction of high risk applicants with verified identities recommended for Known Traveler Number (KTN) denial.	There are a small number of potential applicants that are potentially high risk people. The contractor shall have the ability to identify correctly high risk applicants for specific disqualifying factors, or underlying risk factors for high risk applicants based on the commercial data collected.	<u>Objective</u>: 100% of high risk applicants with verified identities are classified as high risk. <u>Minimum Threshold</u>: z% of high risk applicants with verified identities are classified as high risk.
11. Risk Categorization and Scoring Reconciliation	Risk Threshold Calibration Capability	The contractor shall adjust risk thresholds given additional government furnished information including: Target sensitivity rate Target specificity rate Optimum criterion slope (S) *(If the Government is to create a standard risk score across private sector algorithms, all parties must be able to normalize their risk scores to a standard across the program.)*	The contractor shall be able to calibrate their risk score threshold with a TSA directed risk threshold. If the contractor uses a risk scale of 1-10 with a threshold that states those people above 5 is high risk, and below 5 is low risk is should be able to be calibrated to a TSA risk scale of 1-100 and those above 90 are high risk and below are low risk.	The contractor is capable of calibrating and normalizing their risk threshold based on government furnished information guidance 100% of the time.
12. Risk Categorization and Scoring Reconciliation	Overall Risk Algorithm Performance Compared to Government Set Benchmark	The contractor shall demonstrate the following: Performance that meets or exceeds one or more government set benchmark.	Criteria rationale benchmarks are used.	<u>Objective</u>: Assignment to the highest risk-based prescreening capability level based on statistically outperforming one or more government benchmarks in the government defined operational

				trade space. Minimum Threshold: Assignment to the lowest Risk-Based Prescreening Capability Level based on statistically outperforming one or more government benchmark(s) in the government defined operational tradespace
13. General Algorithm Configuration and Reporting	Continuous Improvement Techniques	The contractor shall demonstrate the ability to: Implement continuous improvement techniques for identity verification and risk algorithm tuning. During periodic continuous improvement testing, outcome data on each of the Contractors (using the metrics above) will be provided to all of the awarded Contractors such that they know their relative performance. No PCII or proprietary information will be disclosed in the process.	The contractor should be able to identify the top and lower tier of rank ordered high and low risk test applicants from the results of the algorithm run. This ranking will allow assessment of future improvements of the version of the algorithm. The disclosure of Contractor performance among all awarded Contractors will allow each Contractor to identify areas for improvement relative to their peers.	The contractor shall document, measure, and report improvements to the identity verification process and Risk Algorithm.
14. General Algorithm Configuration and Reporting	Adaptability to a Changing Threat Environment	The contractor shall demonstrate the following: The ability to adapt to changing threat situations based on government informed threat indicators. *(During the testing phase, contractors will be provided different*	The contractor algorithm shall react to changing threat situation *(using a derogatory category as an indicator)* as directed by TSA. The contractor will also be able to adapt data attribute scoring in response to TSA guidance as required	Objective: The contractor will proactively monitor threat indicators and advise TSA on previously unknown threats. Minimum Threshold: The contractor

		scenarios where a Government informed threat may be used to change the way third parties operate their algorithms. For example, contractors should be able to quickly adopt government restrictions.)	within a set time frame.	shall implement 100% of all government defined threat focus guidance.
15. General Algorithm Configuration and Reporting	Minimum Algorithm Data Inputs	The contractor shall demonstrate: End-to-end enrollment using minimum data elements *(What is the minimum required information from applicants to be able to appropriately establish identity and vet for a KTN?)*	The contractor should, at a minimum, use these data inputs and be ready to explain the use: • Name: first, middle, last name and suffix *(full legal name)* • Date of Birth (DOB) • Address: street, city, state, country; and most recent past address • Gender: Male or Female • Current employer • Names used in the past	100% of applicants with KTN determination using an algorithm and processes that utilize only the minimum government defined data elements.
16. General Algorithm Configuration and Reporting	Algorithm Version Control	The contractor shall demonstrate: Use industry standard audit and version control methods and provide algorithm version information as directed by DHS/TSA *(Have the contractors or their data providers made any changes to the algorithm? If so, what are those changes and what are the potential impacts to operations/security?)*	KTN issuance attributed to private sector algorithm processes must be managed for control, reporting, and auditability.	100% auditability of KTN determination, algorithm version, and supporting data for all records processed through private sector entity systems.
17. General Algorithm	Scalability	The contractor shall demonstrate the ability	The contractor should be able to control the	<u>Objective</u>: The contractor

Configuration and Reporting		to: Control the rate at which pre-screened records are generated through the algorithm.	rate that pre-screened records are produced for enrollment surges and control the rate based on DHS/TSA guidance *(this may be set at an equal rate to the TSA Pre ✓® Application Program or to be able to scale to >10 million in 2 years).*	should be able to process 100,000 pre-screened records within an 8 hour time period through the algorithm. Minimum Threshold: The contractor should be able to process 5,000 pre-screened records within a 4 hour time period through the algorithm.

TSA may wish to work with multiple awarded Contractors to build an "ensemble" method of risk evaluation by passing approved, voluntarily provided records for risk assessments to each Contractor. Such an approach could yield results that are more accurate for both low and high risk than each of the individual Contractors. Each Contractor shall provide back risk scores and then destroy the data after 30 days.

4.11 Key Personnel

The Contractor shall provide qualified staff to perform the functions required. The Contractor shall submit resumes for key personnel to TSA for the approval prior to bringing on board a new individual to fill a key personnel position as defined below:

Positions:
Program Manager
Customer Service Manager
Technical Architect
Personnel Security Manager
Information Systems Security Officer (ISSO)

The Program Manager shall be assigned to the OTA with the responsibility for control and coordination of all work performed. This person shall be the single focal point within the Contractor's organization or team for all tasks and shall be prepared at all times, given reasonable notice, to present and discuss with the Contracting Officer and/or TSA Program Management Office the status of all requirements and problems. For the purposes of this contract, the Contractor's program manager shall be considered a key person.

The Customer Service Manager shall report directly to the Program Manager and be responsible for day-to-day management of customer service capabilities.

The Technical Architect shall report to the Program Manager and be responsible for integrating the Contractor's system with TSA. Integration shall include, but not be limited to, software development and connectivity.

The Personnel Security Manager shall report to the Program Manager shall assist with the Personnel Security administrative and security support services as defined in **Section 4.16**. The Personnel Security Manager shall maintain a database, connecting each individual whom they are responsible for that is transitioning on or off the program, including dates, name, contact information, and clearance status

The Information Systems Security Officer (ISSO)shall report to the Program Manager and be responsible for ensuring that all system security requirements are met, i.e., System Authorization, and System Security Plan.

The Contractor may also propose other key personnel positions with role description for TSA review and approval.

4.12 Risk Management

The Contractor shall be proactive in management of risks, to include the identification and definition of risks, preparation of qualitative risk assessments and risk mitigation considerations to the COR and appropriate Government officials. When identifying risks, the Contractor shall also include cybersecurity risks. The Contractor shall implement all TSA approved risk mitigation requirements.

4.13 Reporting

4.13.1 Monthly Reporting

The Contractor shall provide monthly reports to the COR and other individuals to be identified by TSA upon OTA contract award. The monthly reports should address the previous month's activities. In conjunction with the monthly status report, the Contractor shall conduct monthly Program Management Reviews (PMR) to present to the Government. The PMR shall include the critical information on the program status and projected progress and performance. The monthly reports should provide a status for the following information:

- Major activities
- Completed activities
- Pending issues and activities
- System and process changes
- Operational metrics showing program trends for each module in the system, to included but not limited to, the following:
    - Number of applications processed, per month, per enrollment center, and cumulative;
    - Number of applications submitted to TSA per month
    - Number of applications not submitted to TSA per month

  - Of the applications not submitted to TSA, the number of individuals who applied for redress
  - Of the applications not submitted to TSA, the number that were not submitted due to failure of the identity assurance process (as defined in **Section 4.2**)
  - Of the applications not submitted to TSA, the number that were not submitted due to failure of the eligibility evaluation (as defined in **Section 4.3**)
- Funds reconciliation report
- Customer service metrics to include reporting on number of inquiries and AQLs
- Status of applicant enrollment marketing and outreach efforts
- Mobile enrollment events
- Number of security or privacy incidents for the month
- IT required metrics such as POA&Ms and software upgrades
- Performance metrics as defined by the SLAs. Please see section 4.10 for performance measures that require monthly reporting.

4.13.2 Ad-Hoc Reporting

The Contractor shall provide to TSA ad-hoc reporting and metrics such as but not limited to demographic information.

4.14 IT and System Security Requirements

4.14.1Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to Government Off the Shelf (GOTS) and Commercial Off the Shelf (COTS) software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available which meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this

standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

4.14.2 DHS and TSA Enterprise Architecture Compliance

a) The Contractor shall ensure that all solutions, products, deliverables, and services are aligned and compliant with the current DHS and TSA Enterprise Architecture, and the Federal Enterprise Architecture Framework (OMB Reference Models).

b) All solutions and services shall meet DHS and TSA Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with Homeland Security Enterprise Architecture (HLS EA) requirements.
   i. All developed solutions and requirements shall be compliant with the HLS EA.
   ii. The contractor shall align all solutions and services and ensure compliance with applicable TSA and DHS IT Security, Application, System, Network, Data, Information, and Business Architecture policies, directives, guidelines, standards, segment architectures and reference architectures.
   iii. The contractor shall utilize any existing TSA or DHS user interface design standards, style guides, and/or policies and standards for human factors, usability, user experience, or human computer interaction (HCI).
   iv. All solution architectures and services (Application, System, Network, Security, Information, etc.) shall be reviewed and approved by TSA EA as part of the TSA SELC review process and in accordance with all applicable DHS and TSA IT governance policies, directives, and processes (i.e. TSA IT Governance Management Directive 1400.20). This includes the Solution Engineering Review (SER), Preliminary Design Review (PDR) and Critical Design Review (CDR) stage gates. All implementations shall follow the approved solution architecture/design without deviation. Any changes, to either the prior approved solution and/or prior approved design that are identified during subsequent SELC phases, including testing, implementation and deployment, shall undergo additional EA review prior to proceeding.
   v. All IT hardware and software shall be compliant with the TSA and HLS EA Technical Reference Model (TRM) Standards and Products Profile; all products are subject to TSA and DHS Enterprise Architectural approval. No products may be utilized in any production environment that is not included in the TSA and HLS EA TRM Standards and Products Profile.

c) Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the TSA

Enterprise Architecture Data Management Team, who will be responsible for coordination with the DHS Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

i. Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS and TSA data management architectural guidelines and subject to the TSA Enterprise Architecture Data Management Team (EDM) approval.

ii. In addition to the Federal Acquisitions Regulations (FAR) Subpart 27.4 – 'Rights in Data and Copyrights' and Section 35.011 detailing technical data delivery, the contractor shall provide all TSA-specific data in a format maintaining pre-existing referential integrity and data constraints, as well as data structures in an understandable format to TSA. Examples of data structures can be defined as, but not limited to
    a. Data models depicting relationship mapping and, or linkages
    b. Metadata information to define data definitions
    c. Detailed data formats, type, and size
    d. Delineations of the referential integrity (e.g., primary key/foreign key) of data schemas, structures, and or taxonomies

iii. All TSA-specific data shall be delivered in a secure and timely manner to TSA. Data security is defined within the 'Requirements for Handling Sensitive, Classified, and/or Proprietary Information', section of this SOW. This definition complies with not only the delivery of data, but also maintaining TSA-specific data within a non-TSA or DHS proprietary system. Alternative data delivery techniques may also be defined by TSA Enterprise Data Management (EDM) team.

iv. All metadata shall be pre-defined upon delivery to TSA. Metadata shall be delivered in a format that is readily interpretable by TSA (e.g. metadata shall be extracted from any metadata repository that is not utilized by TSA and delivered in a TSA approved manner). Metadata shall also provide an indication of historical verses the most current data to be used, as well as frequency of data refreshes.

v. The contractor shall adhere to providing a Data Management Plan (DMP), as defined by Enterprise Architecture, to the EA design review team before the preliminary/critical design review. The Data Management Plan includes conceptual and logical data models, data dictionaries, data asset profile, and other artifacts pertinent to the project's data. All data artifacts must adhere to TSA EA data standards defined and published before the design review. Data Standards include but are not limited to, data asset standards, metadata standards, logical/physical naming standards, and information exchange (using the National Information Exchange Model (NIEM)) standards. All required artifacts must be provided to and approved by the EA Design Review team.

d) Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

4.14.3 IT System Security Requirements

A. Controls

A.1. The Contractor shall comply with Department of Homeland Security (DHS) and Transportation Security Administration (TSA) technical, management and operational security controls to ensure that the Government's security requirements are met. These controls are described in DHS PD 4300A and TSA MD 1400 series security policy documents and are based on the NIST Special Publication (SP) 800-53 standards.

A.2. The Contractor shall include this prospective clause in all subcontracts at any tier where the subcontractor may have access to "sensitive information" as defined in this prospective clause.

B. General Security Responsibilities for Contract Performance

B.1. The Contractor shall ensure that its employees follow all policies and procedures governing physical, environmental, and information security described in the various TSA regulations pertaining thereto, good business practices, and the specifications, directives, and manuals for conducting work to generate the products as required by this contract. Personnel will be responsible for the physical security of their area and government furnished equipment (GFE) issued to them under the provisions of the contract.

B.2. All Contractor employees shall receive initial TSA IT Security Awareness Training within 60 days of assignment to the contract.

B.3. Refresher training must be completed annually thereafter.

B.4. Role Based training for contract employees individuals with Significant Security Responsibility (SSR), whose job proficiency is required for overall network security within TSA, will be in accordance with DHS and TSA policy.

B.5. Individuals with SSR will have a documented individual training and education plan, which will ensure currency with position skills requirements, with the first course to be accomplished within 90 days of employment or change of position. The individual training plan will be refreshed annually or immediately after a change in the individual's position or related position description requirements.

B.6. The education and training will meet standards established by the National Institute of Standards and Technology (NIST) and set forth in DHS and TSA security policy.

B.7. Evidence of training provided to personnel will be available upon request of the DHS IT Security Training Office, or during DHS/TSA onsite validation visits performed on a periodic basis.

C. Configuration Management (hardware/software)

C.1. Hardware or software configuration changes shall be in accordance with the DHS Information Security Performance Plan (current year and any updates thereafter), the DHS Continuous Diagnostics and Mitigation (CDM) Program to include dashboard reporting requirements and TSA's Configuration Management policy. The TSA Chief Information Security Officer (CISO)/ Information Assurance and Cyber Security Division (IAD) must be informed of and involved in all configuration changes to the TSA IT environment including systems, software, infrastructure architecture, infrastructure assets, and end user assets. The TSA IAD will approve any request for change prior to any development activity occurring for that change and will define the security requirements for the requested change.

C.2. The Contractor shall ensure all application or configuration patches and/or Request for Change (RFC) have approval by the Technical Discussion Forum (TDF), and Systems Configuration Control Board (SCCB) and lab regression testing prior to controlled change release under the security policy document, TSA Management Directive (MD) 1400.3 and TSA Information Assurance Handbook, unless immediate risk requires immediate intervention. Approval for immediate intervention (emergency change) requires approval of the TSA CISO, SCCB co-chairs, and the appropriate Operations Manager, at a minimum.

C.3. The Contractor shall ensure all sites impacted by patching are compliant within 14 days of change approval and release.

C.4. The acquisition of commercial-off-the-shelf (COTS) Information Assurance (IA) and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting "sensitive information") shall be limited to those products that have been evaluated and validated, as appropriate, in accordance with the following:

- The NIST FIPS validation program.
- The National Security Agency (NSA)/National Institute of Standards and Technology (NIST) National Information Assurance Partnership (NIAP) Evaluation and Validation Program.
- The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement.

C.5. US Government Configuration Board and DHS Configuration Guidance

a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the US Government Configuration Board (USGCB) and in accordance with DHS and TSA guidance.
    1. USGCB Guidelines:
        a. http://usgcb.nist.gov/usgcb_content.html
    2. DHS Sensitive Systems Configuration Guidance
        a. http://dhsconnect.dhs.gov/org/comp/mgmt/cio/iso/Pages/sscg.aspx

b) The standard installation, operation, maintenance, updates and/or patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

C.6. The Contractor shall establish processes and procedures for continuous monitoring of Contractor systems that contain TSA data by ensuring all such devices are monitored by, and report to, the TSA Security Operations Center (SOC).

D. Risk Management Framework

D.1. The Security Authorization and Ongoing Authorization Process in accordance with NIST SP 800-37 and SP 800-137 (current versions) is a requirement for all TSA IT systems, including general support systems (e.g., standard TSA desktop, general network infrastructure, electronic mail, etc.), major applications and development systems (if connected to the operational network or processing, storing, or transmitting government data). These processes are documented in the NIST Risk Management Framework. Ongoing Authorization is part of Step 6 "Monitoring" of the Risk Management Framework. All NIST and DIACAP guidance are publicly available; TSA and DHS security policy is disclosed upon contract award.

D.2. A written authority to operate (ATO) granted by the TSA Authorizing Official (AO) is required prior to processing operational data or connecting to any TSA network. The contractor shall provide all necessary system information for the security authorization effort.

D.3. TSA will assign a security category to each IT system compliant with the requirements of Federal Information Processing Standards (FIPS) 199 and assign security controls to those systems consistent with FIPS 200.

D.4. Unless the AO specifically states otherwise for an individual system, the duration of any Accreditation will be dependent on the FIPS 199 rating and overall residual risk of the system; the length can span up to 36 months.

D.5. The Security Authorization Package contains documentation required for Security Authorizations and Ongoing Authorization. The package shall contain the following security documentation: 1) Security Assessment Report (SAR) 2) Security Plan (SP) or System Security Authorization Agreement (SSAA), 3) Contingency Plan, 4) Contingency Plan Test Results, 5) Federal Information Processing Standards (FIPS) 199 Security Categorization, 6) Privacy Threshold Analysis (PTA), 7) E-Authentication, 8) Security Assessment Plan (SAP), 9)Authorization to Operate (ATO) Letter, 10) Plan of Action and Milestones (POA&M), and 11) Ongoing Authorization Artifacts as required by the DHS Ongoing Authorization Methodology (current version). The SA package shall document the specific procedures, training, and accountability measures in place for systems that process personally identifiable information (PII). All security compliance documents will be reviewed and approved by the Chief Information Security Officer (CISO) and the Information Assurance and Cyber Security Division (IAD), and accepted by the Contracting Officer upon creation and after any subsequent changes, before they go into effect.

E. Contingency Planning

E.1. The Contractor shall develop and maintain a Contingency Plan (CP), to include a Continuity of Operation Plan (COOP), to address circumstances whereby normal operations are disrupted in accordance with The Office of Management and Budget (OMB) Circular A-130, Appendix III.

E.2. The Contractor shall ensure that contingency plans are consistent with template provided in the DHS Information Assurance Compliance System Tool. If access has not been provided initially, the contractor shall use the DHS 4300A Sensitive System Handbook, Attachment K, IT Contingency Plan Template.

E.3. The Contractor shall identify and train all TSA personnel involved with COOP efforts in the procedures and logistics of the disaster recovery and business continuity plans.

E.4. The Contractor shall ensure the availability of critical resources and facilitate the COOP in an emergency situation.

E.5. The Contractor will test their CP annually.

E.6. The Contractor shall record, track, and correct any CP deficiency and any deficiency correction that cannot be accomplished within one month of the annual test will be elevated to the Information Assurance and Cyber Security Division (IAD).

E.7. The Contractor shall retain records of the annual CP testing for review during periodic audits.

E.8. The Contractor shall ensure the CP addresses emergency response, backup operations, and recovery operations.

E.9. The Contractor shall have an Emergency Response Plan that includes procedures appropriate to fire, flood, civil disorder, disaster, bomb threat, or any other incident or activity that may endanger lives, property, or the capability to perform essential functions.

E.10. The Contractor shall have a Backup Operations Plan that includes procedures and responsibilities to ensure that essential operations can be continued if normal processing or data communications are interrupted for any reason for an unacceptable period of time as described in the Statement of Work.

E.11. The Contractor shall have a Post-disaster Recovery Plan that includes procedures and responsibilities to facilitate rapid restoration of normal operations at the primary site or, if necessary, at a new facility following the destruction, major damage, or other major interruption at the primary site.

E.12. The Contractor shall ensure all TSA data (e.g., mail, data servers, etc.) is incrementally backed up on a daily basis.

E.13. The Contractor shall ensure a full backup of all network data occurs as required by the system's availability security categorization impact rating per TSA Information Assurance policy.

E.14. The Contractor shall ensure all network application assets (e.g., application servers, domain controllers, Information Assurance (IA) tools, etc.) will be incrementally backed up as required to eliminate loss of critical audit data and allow for restoration and resumption of normal operations within one hour.

E.15. The Contractor shall ensure sufficient backup data to facilitate a full operational recovery within one business day at either the prime operational site or the designated alternate site will be stored at a secondary location determined by the local element disaster recovery plan.

E.16. The Contractor shall ensure that data at the secondary location is current as required by the system's availability security categorization impact rating.

E.17. The Contractor shall ensure the location of the local backup repository and the secondary backup repository is clearly defined, and access controlled as an Information Security Restricted Area (ISRA).

E.18. The Contractor shall adhere to the DHS Security Architecture Guidance Volume 1: Network and System Infrastructure for the layout of the file systems, or partitions, on a system's hard disk impacting the security of the data on the resultant system. File system design shall:

- Separate generalized data from operating system (OS) files
- Compartmentalize differing data types
- Restrict dynamic, growing log files or audit trails from crowding other data.

E.19. The contractor shall adhere to the DHS Security Architecture Guidance Volume 1: Network and System Infrastructure Design for the management of mixed data for OS files, user accounts, externally-accesses data files and audit logs.

F. Program Performance

F.1. The Contractor shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA Information Assurance and Cyber Security Division (IAD) and management, as directed by the Contracting Officer.

F.2. The Contractor shall provide support during the Information Assurance and Cyber Security Division (IAD) audit activities and efforts. These audit activities may include, but are not limited to the following: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

G. Federal Risk and Authorization Management Program (FedRAMP)
If a vendor is to host a system with a Cloud Service Provider, the following shall apply:

G.1. FedRAMP Requirements: Private sector solutions will be hosted by a Joint Authorization Board (JAB) approved Infrastructure as a Service (IaaS) Cloud Service Provider (CSP) (http://cloud.cio.gov/fedramp/cloud-systems) and shall follow the Federal Risk and Authorization Management Program (FedRAMP) requirements. The Cloud Service Provider shall adhere to the following in addition to the FedRAMP requirements: Identity and entitlement access management shall be done through Federated Identity; SSI and PII shall be encrypted in storage and in transit as it is dispersed across the cloud; Sanitization of all TSA data shall be done as necessary at the IaaS, PaaS or SaaS levels; Cloud bursting shall not occur; TSA data shall be logically separated from other cloud tenants; All system administrators shall be U.S. citizens; TSA data shall not leave the United States; The cloud internet connection shall be behind a commercial Trusted Internet Connection that has EINSTEIN 3 Accelerated (E3A) capabilities deployed. These include but are not limited to the analysis of network flow records, detecting and alerting to known or suspected cyber threats, intrusion prevention capabilities and under the direction of DHS detecting and blocking known or suspected cyber threats using indicators. The E3A capability shall use the Domain Name Server Sinkholing capability and Email filtering capability allowing scans to occur destined for .gov networks for malicious

attachments, Uniform Resource Locators and other forms of malware before being delivered to .gov end-users.

G.2. Private Sector System Requirements: TSA shall conduct audits at any time on the private sector systems, and the system shall be entered into the TSA FISMA Inventory as a system of record using the Control Implementation Summary (CIS) provided by the Cloud Service Provider. Security artifacts shall be created and maintained in the DHS Information Assurance Compliance Tool (IACS). The private sector systems are required to go through the Security Authorization Process and the Risk Management Framework in accordance the Federal Information Systems Management Act and NIST SP 800-37 Rev. 1. The cloud internet connection shall be behind a commercial Trusted Internet Connection that has EINSTEIN 3 Accelerated (E3A) deployed. Security event logs and application logs shall be sent to the TSA SOC. Incidents as defined in the TSA Information Assurance 1400.3 Management Directive and Handbook shall be reported to the TSA SPOC 1-800-253-8571. DHS Information Security Vulnerability Management Alerts and Bulletins shall be patched within the required time frames as dictated by DHS.

H. Information Assurance Policy

H.1. All services, hardware and/or software provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy Directive, DHS 4300A Sensitive Systems Handbook., TSA MD 1400.3 Information Technology Security Policy, TSA Information Assurance Handbook and Technical Standards.

H.2. The Contractor solution shall follow all current versions of TSA and DHS policies, procedures, guidelines, and standards, which will be provided by the Contracting Officer, including but not limited to:

- DHS Sensitive Systems Policy Directive (PD) 4300A
- DHS 4300A Sensitive Systems Handbook
- DHS National Security Systems Policy Directive (PD) 4300B
- DHS 4300B National Security Systems Handbook·
- TSA MD 1400.3 Information Technology Security
- TSA Information Assurance Handbook
- TSA Technical Standards
- DHS IT Security Architecture Guidance Volumes 1, 2 and 3
- DHS/TSA Systems Engineering Lifecycle (SELC)
- DHS Performance Plan (current fiscal year)
- DHS Ongoing Authorization Methodology (current version)
- OMB M-10-28, M-14-03

H.3. Authorized use of TSA IT systems and resources shall be in accordance with the TSA Information Assurance Handbook.

H.4. The contractor shall complete TSA Form 251 and TSA Form 251-1 for sensitive or accountable property. The contractor shall email the completed forms to TSA-Property@dhs.gov and include a hard copy with the shipment.

I. Data Stored/Processed at Contractor Site

I.1. Unless otherwise directed by TSA, any storage of data must be contained within the resources allocated by the Contractor to support TSA and may not be on systems that are shared with other commercial or government clients.

J. Remote Access

J.1. The Contractor remote access connection to TSA networks shall be considered a privileged arrangement for both Contractor and the Government to conduct sanctioned TSA business. Therefore, remote access rights must be expressly granted, in writing, by the TSA Information Assurance and Cyber Security Division (IAD).

J.2. The Contractor remote access connection to TSA networks may be terminated for unauthorized use, at the sole discretion of TSA.

K. Interconnection Security Agreement

If the service being supplied requires a connection to a non-DHS, Contractor system, or DHS system of different sensitivity, the following shall apply:

K.1. Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding/agreement, service level agreements or interconnection service agreements.

K.2. ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.

K.3. ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.

L. SBU Data Privacy and Protection

L.1. The contractor must satisfy requirements to work with and safeguard Sensitive Security Information (SSI), and Personally Identifiable Information (PII). All support personnel must understand and rigorously follow DHS and TSA requirements, policies, and procedures for safeguarding SSI and PII. Contractor personnel will be required to complete online training for SSI and Informational Security, which take one hour each, as well as TSA online Privacy training.

L.2. The Contractor shall be responsible for the security of i) all data that is generated by the contractor on behalf of the TSA, ii) TSA data transmitted by the contractor, and iii) TSA data otherwise stored or processed by the contractor regardless of who owns or controls the underlying systems while that data is under the contractor's control. All TSA data, including but not limited to PII, sensitive security information (SSI), sensitive but unclassified (SBU), and critical infrastructure information (CII), shall be protected according to DHS and TSA security policies and mandates.

L.3. TSA will identify IT systems transmitting unclassified/SSI information that will require protection based on a risk assessment. If encryption is required, the following methods are acceptable for encrypting sensitive information:

FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2. (current version)

National Security Agency (NSA) Type 2 or Type 1 encryption. (current version)

Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) 4300A Sensitive Systems Handbook). (current version)

L.4. The contractor shall maintain data control according to the TSA security level of the data. Data separation shall include the use of discretionary access control methods, VPN encryption methods, data aggregation controls, data tagging, media marking, backup actions, and data disaster planning and recovery. Contractors handling PII must comply with TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information* (current version).

L.5. Users of TSA IT assets shall adhere to all system security requirements to ensure the confidentiality, integrity, availability, and non-repudiation of information under their control. All users accessing TSA IT assets are expected to actively apply the practices specified in the TSA Information Assurance Handbook and applicable IT Security Technical Standards.

L.6. The contractor shall comply with Sensitive Personally Identifiable Information (Sensitive PII) disposition requirements stated in the TSA Information Assurance Handbook, applicable Technical Standards and TSA MD 3700.4, *Handling Sensitive Personally Identifiable Information*.

L.7. The Contractor shall ensure that source code is protected from unauthorized access or dissemination.

M. Disposition of Government Resources

M.1 At the expiration of the contract, the contractor shall return all TSA information and IT resources provided to the contractor during the contract, and provide a certification that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.3, TSA Information Assurance Handbook and Technical Standards. The contractor shall certify in writing that sanitization or destruction has been performed. Sanitation and destruction methods are outlined in the NIST Special Publication 800-88 Guidelines for Media Sanitization, and TSA Technical Standard 046 *IT Media Sanitization and Disposition*. The contractor shall email signed proof of sanitization to the COTR. In addition, the contractor shall provide a master asset inventory list that reflects all assets, government furnished equipment (GFE) or non-GFE that were used to process TSA information.

N. Special Considerations and Circumstances (if applicable)

Security Program Plan

N.1 For major agency Information Technology (IT) infrastructure support ranging in the total estimated procurement value (TEPV) of about $100 million or above **or** per TSA management's request, the contractor may need to provide, implement, and maintain a Security Program Plan (SPP) based on the templates provided by the TSA Information Assurance and Cyber Security Division (IAD). This plan shall describe the processes and procedures that will be followed to ensure the appropriate security of IT resources that are developed, processed, or used under this contract. At a minimum, the contractor's SPP shall address the contractor's compliance with the controls described in NIST SP 800-53 (current version). The security controls contained in the plan shall meet the

requirements listed in the TSA Information Assurance Handbook, Technical Standards and the DHS Sensitive Systems Policy Directive and Handbook 4300A (current versions).
N.2 The SPP shall be a living document. It will be reviewed and updated semi-annually to address new processes, procedures, technical or federally mandated security controls and other contract changes that affect the security of IT resources under contract.
N.3 The SPP shall be submitted within 30 days after contract award. The SPP shall be consistent with and further detail the approach contained in the offeror's proposal or quote that resulted in the award of this contract and in compliance with the requirements stated in this clause.
N.4 The SPP, as accepted by the Contracting Officer and Information System Security Officer (ISSO), shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

O. Security Authorization (C&A)

The Security Authorization Process in accordance with the National Institute of Standards and Technology (NIST) 800-37 (current version) for unclassified systems, or the Department of Defense (DoD) Information Assurance Security Authorization Process (DIACAP) for classified systems, is a requirement for TSA information systems, including general support systems (e.g., standard TSA desktop, general network infrastructure, electronic mail, etc.), major applications and development systems (if connected to the operational network or processing, storing, or transmitting government data). All NIST and DIACAP guidance are publicly available; TSA and DHS security policy is disclosed upon OTA award. A written authority to operate (ATO), granted by the TSA Authorizing Official (AO), is required prior to processing operational data or connecting to any TSA network. The contractor shall provide all necessary system information for the security authorization effort.

Within 45 days of contract award, the Contractor shall be able to begin Security Authorization activities. Within 60 days of the start of the testing described in Section 4.4, the Contractor shall complete all activities necessary to receive ATO. The Security Authorization Package contains documentation required for security authorization. The package will contain the following security documentation: 1) Security Assessment Report (SAR) 2) System Security Plan (SSP) or System Security Authorization Agreement (SSAA), 3) Contingency Plan, 4) Contingency Plan Test Results, 5) Federal Information Processing Standards (FIPS) 199 Categorization, 6) Privacy Threshold Analysis (PTA), 7) E-Authentication,

8) Security Test and Evaluation (ST&E) Plan, 9) Authorization to Operate (ATO) Letter, 10) Plan of Action and Milestones (POA&M), and 11) Annual Assessments. The Security Authorization package shall document the specific procedures, training, and accountability measures in place for systems that process personally identifiable information (PII) and sensitive security information (SSI). All security compliance documents will be reviewed and approved by the Chief Information Security Officer (CISO) and the Information Assurance and Cyber Security Division (IAD), and accepted by the Contracting Officer upon creation and after any subsequent changes, before they go into effect.

The Contractor shall comply with requests to be audited and provide responses within three business days to requests for data, information, and analysis from the TSA Information Assurance and Cyber Security Division (IAD) and management, as directed by the Contracting Officer.

Access to Unclassified Facilities, Information Technology Resources, and Sensitive Information

The assurance of the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance are essential to the DHS mission. DHS Management Directive (MD) 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information, describes how contractors must handle sensitive but unclassified information. DHS MD 4300.1 Information Technology Systems Security and the DHS Sensitive Systems Handbook prescribe policies and procedures on security for IT resources. Contractors shall comply with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically for all Task Orders that require access to DHS facilities, IT resources or sensitive information. Contractors shall not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the task order.

Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the COR, TSA program manager and the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of g o v e r n m e n t oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 5.5, September 30, 2007) or any replacement

publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

CONTRACTOR EMPLOYEE ACCESS

(a) *Sensitive Information*, as used in this Chapter, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

(b) “Information Technology Resources” include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

(e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer’s Technical Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the

individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;

(2) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(3) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the contracting officer.

(End of clause)

Special Information Technology Contract Security Requirements

(a) Identification Badges. All Contractor employees shall be required to obtain and wear TSA identification badges when working in TSA facilities.

(b) Computer Access Agreement. All Contractor employees (users, managers, and operators of the TSA network) must sign TSA Form 1403, *Computer Access Agreement.* A copy of which shall be provided to the TSA contracting officer's technical representative for retention for the duration of the contract.

(c) OTA Contractor Personnel Security.

(1) Privileged access users are individuals who have access to an information technology (IT) system with privileges of Administrator or above and have access to sensitive network infrastructure data. Privileged access users will be appropriately screened on entry into the privileged access position and the initial screening shall be refreshed every two years,

(2) Individuals terminating voluntarily or involuntarily from a Contractor performing under contract at TSA must have an exit briefing, conducted by a supervisory or management-level employee of the Contractor in order to identify and explain their post- employment responsibilities to the TSA.

(3) Records of exit interviews will be signed and maintained by the Contractor as part of the individual employment record for a period of not less than two years following the termination of the individual's employment.

(4) The Contractor shall notify the Contracting Officer's Technical Representative and the Contracting Officer with proposed personnel changes. Written confirmation is required. This includes, but is not limited to, name changes, resignations, terminations, and reassignments to another contract.

(5) The Contractor shall notify the TSA, in writing of any requested change in access requirements for its employees no later than one day after any personnel changes occur. This includes name changes, resignations, terminations, and transfers to other company engagements. The Contractor shall provide the following information to TSA: full name, social security number, effective date, and reason for change.

(6) The Contracting Officer must approve all personnel replacements. Estimated completion of the necessary background investigation for employee access to government facilities and information systems is approximately 30 days from the date the completed forms are received (and acknowledged as complete) in the Security Programs Division.

(7) Failure of any Contractor personnel to pass a background investigation, without timely substitution that meets the contracts requirements, may be grounds for termination of the contract.

(d) Non-Disclosure Agreements.

(1) All TSA contractor employees and consultants must execute a DHS Form 11000-6, *Sensitive But Unclassified Information Non-Disclosure Agreement (NDA)* upon initial assignment to TSA and before being provided access to TSA "sensitive and/or mission critical information." The original NDA will be provided to the TSA contracting officer's technical representative for retention for the duration of the contract.

(2) The Contractor, and those operating on its behalf, shall adhere to the requirements of the nondisclosure agreement unless otherwise authorized in writing by the Contracting Officer.

(e) Performance Requirements.

(1) The Contractor shall not be liable for any injury to Government personnel or damage to Government property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

(2) Contracting Officer's Representative (COR) and IT Security Division shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

4.14.4 Operations and System Maintenance

The Contractor shall provide operational support of system hardware configurations and shall monitor operating system and application software operations to ensure ongoing, continuous operation is maintained. Physical and logical network management support including, but not be limited to, session awareness, traffic flow visibility, failure notification shall be provided. The Contractor shall support problem identification, detection and isolation, perform reconfiguration, troubleshooting, diagnostics/remedial action, as needed to ensure end-to-end physical connectivity and operations.

The Contractor shall operate the system in accordance with the requirements detailed in the SOW. This includes support and repair for the OTA Contractor's system software, hardware, network infrastructure, and all tasks associated with the system Continuity of Operations Plan (COOP). In providing operations and maintenance of the system the Contractor shall address the following:

- The storage and filing of biographic, biometric (at a minimum fingerprint), and identity documents collected.
- The establishment and operation of 24 hours a day, 7 days a week system availability as defined in Section 4.10.1;
- Operations and maintenance of the OTA contractor's system to include all technical requirements listed in Section 4.0 and Attachment #1 - TSA Pre✓ ® Application Expansion High Level Requirements;
- Roll-up and report generation of performance metrics for the program;
- Maintenance of the chain of trust for applicant's data and information, and
- Provide problem analysis and resolution of system and mission-specific infrastructure configuration problems, to include application of fixes to resolve problems identified during production operations or testing,
- Providing coordination and assistance to TSA program staff, vendors, and other contractors or parties authorized by TSA in resolving system and mission-specific infrastructure hardware, software, or network problems.

The Contractor shall provide a scheduled maintenance program. Maintenance support shall be provided for all hardware and software, inclusive of existing and any new equipment or products introduced during performance to keep pace with changing technology. All hardware support and spare parts required shall be provided as a part of this service by the Contractor. The Contractor shall install/test/maintain software, upgrades or modifications; and perform automated patch management and version control of all products.

Unscheduled maintenance actions shall be communicated immediately and directly to COR and TSA program management office.

The Contractor shall document and implement an incident response plan (IRP) that includes notification to TSA. Incidents must be reported to TSA immediately. The Contractor shall perform IR follow up actions as requested by TSA.

When maintaining the system, the Contractor shall apply sound operational and maintenance engineering processes and procedures; follow rigid controls in implementing hardware and software upgrades into the operational environment; update documentation affected by changes; and ensure that upgrade/modifications of software are stable and backup is maintained.

The Contractor shall implement an automated configuration change control management process using TSA approved COTS/GOTS.

4.14.5 System Security Requirements

- The Contactor's system must be built on a Joint Accreditation Board (JAB) approved Federal Risk and Authorization Management Program (FEDRAMP) Cloud, FEDRAMP Cloud with an Agency Authority to Operate (ATO), or be on a General Support System that currently has an ATO from another Federal Entity. The Cloud or General Support System will be authorized at the M/M/M Level.
    - If a Security Authorization from another Federal Entity is used, TSA must be provided the full Authorization Package
- The Contractor's system will be considered a Major Application sitting on the General Support System that was previously ATO'd by the Fedramp JAB, Fedramp Agency ATO, or another Federal Agency. The private screening system Major Application will become a system within TSA's System Inventory.
- The enrollment stations and any other systems used in the field will be part of the System Boundary of the Major Application.
- The Contractor's Major Application will be accredited and authorized to operate by TSA at the M/M/M level
- TSA PIV card use by all vendor personnel to access the enrollment machines (IT Security Phase III- 9 months from OTA award)

- All traffic passing into and out of the MA/Cloud or MA/General Support System to and from the Internet must be routed through a MTIPS (Managed Trusted Internet Protocol Service) TIC Vendor that has Einstein E3A implemented. (IT Security Phase II- 3 months from OTA award).
- All vendor personnel with access to TSA Data or Systems will have a Background Investigation performed by TSA Personnel Security prior to access being granted; All personnel including system administrators must be US citizens;
- All TSA data shall be located in the United States.
- The Contractor will implement TSA's privileged account process for the management of all privileged accounts. These accounts are audited yearly by TSA.
- The Contractor will use .gov domain names.
- During testing and evaluation (T&E), the TSA shall conduct cyber red-teaming of the Contractor solution to identify cyber vulnerabilities. In particular, emphasis will be placed on maintaining the confidentiality and integrity of the PII data and their associated KTNs. Once a Contractor has received clearance to move into operations, red-teaming will continue with the Contractors as part of continuous improvement.

4.14.6 Security of Systems Handling Personally Identifiable Information and Privacy Incident Response

(a) Definitions.

"Breach" (may be used interchangeably with "Privacy Incident') as used in this clause means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar situation where persons other than authorized users, and for other than authorized purpose, have access or potential access to Personally Identifiable Information, in usable form whether physical or electronic.

"Personally Identifiable Information (PII)" as used in this clause means any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to that individual regardless of whether the individual is a citizen of the United States, legal permanent resident, or a visitor to the United States.

Examples of PII include: name, date of birth, mailing address, telephone number, Social Security Number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), Internet protocol addresses, biometric identifiers (e.g., fingerprints), photographic facial Images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Personally Identifiable Information (Sensitive PII)" as used in this clause is a subset of Personally Identifiable Information, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. , Complete social security numbers (SSN), alien registration numbers (A-number) and biometric identifiers (such as fingerprint, voiceprint, or iris scan) are considered Sensitive PII even if they are not coupled with additional PII. Additional examples include any groupings of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(1) Driver's license number, passport number, or truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Financial information such as account numbers or Electronic Funds Transfer Information
(5) Medical Information
(6) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other Personally Identifiable information may be "sensitive" depending on its context, such as a list of employees with less than satisfactory performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains Personally Identifiable Information but it is not sensitive.

(b) Systems Access. Work to be performed under this contract requires the handling of Sensitive PII. The contractor shall provide the Government access to, and information regarding systems the contractor operates on behalf of the Government under this contract, when requested by the Government, as part of its responsibility to ensure compliance with security requirements, and shall otherwise cooperate with the Government in assuring compliance with such requirements. Government access shall include independent validation testing of controls, system penetration testing by the Government, Federal Information Security Management Act (FISMA) data reviews, and access by agency Inspectors General for its reviews.

(c) Systems Security. In performing its duties related to management, operation, and/or access of systems containing Sensitive PII under this contract, the contractor, its employees and subcontractors shall comply with applicable security requirements described in DHS Sensitive System Publication 4300A or any replacement publication and rules of conduct as described in TSA MD 3700.4¬

In addition, use of contractor-owned laptops or other media storage devices to process or store PII is prohibited under this contract until the contractor provides, and the Contracting officer in coordination with CISO approves written certification by the contractor that the following requirements are met:

(1) Laptops employ encryption using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;

(2) The contractor has developed and implemented a process to ensure that security and other applications software are kept current;

(3) Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;

(4) When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS security requirements.

(5) The contractor shall maintain an accurate inventory of devices used in the performance of this contract;

(6) Contractor employee annual training and rules of conduct/behavior shall be developed, conducted/issued, and acknowledged by employees in writing. Training and rules of conduct shall address at minimum:
(i) Authorized and official use;
(ii) Prohibition against use of personally-owned equipment to process, access, or store Sensitive PII;
(iii) Prohibition against access by unauthorized users and unauthorized use by authorized users; and
(iv) Protection of Sensitive PII;

(7) All Sensitive PII obtained under this contract shall be removed from contractor-owned information technology assets upon termination or expiration of contractor work. Removal must be accomplished in accordance with DHS Sensitive System Publication 4300A, which the contracting officer will provide upon request. Certification of data removal will be performed by the contractor's Project Manager and written notification confirming certification will be delivered to the contracting officer within 15 days of termination/expiration of contractor work.

(d) Data Security. Contractor shall limit access to the data covered by this clause to those employees and subcontractors who require the information in order to perform their official duties under this contract. The contractor, contractor employees, and subcontractors must physically secure Sensitive PII when not in use and/or under the control of an authorized individual, and when in transit to prevent unauthorized access or loss. When Sensitive PII is no longer needed or required to be retained under applicable Government records retention policies, it must be destroyed through means that will make the Sensitive PII irretrievable.

The contractor shall only use Sensitive PII obtained under this contract for purposes of the contract, and shall not collect or use such information for any other purpose without the prior written approval of the contracting officer. At expiration or termination of this

contract, the contractor shall turn over all Sensitive PII obtained under the contract that is in its possession to the Government.

(e) Breach Response. The contractor agrees that in the event of any actual or suspected breach of Sensitive PII (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), it shall immediately, and in no event later than one hour of discovery, report the breach to the contracting officer, the Contracting Officer's Technical Representative (COTR), and the TSA Director of Privacy Policy & Compliance (TSAprivacy@dhs.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties.

(f) Personally Identifiable Information Notification Requirement. The contractor has in place procedures and the capability to promptly notify any individual whose Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate. The method and content of any notification by the contractor shall be coordinated with, and subject to the prior approval of the Government, based upon a risk-based analysis conducted by the Government in accordance with DHS Privacy incident Handling Guidance. Notification shall not proceed unless the Government has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to Government 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 the Government. 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.

In the event that a Sensitive PII breach occurs as a result of the violation of a term of this contract by the contractor or its employees, the contractor shall, as directed by the contracting officer and at no cost to the Government, 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 12 months from discovery of the breach. Should the Government elect to provide and/or procure notification or identity protection services in response to a breach, the contractor will be responsible for reimbursing the Government for those expenses.

(g) Pass-Through of Security Requirements to Subcontractors. The contractor agrees to incorporate the substance of this clause, its terms and requirements, in all subcontracts under this contract, and to require written subcontractor acknowledgement of same.

Violation by a subcontractor of any provision set forth in this clause will be attributed to the contractor.

4.15 Deliverables

The Contractor shall coordinate with the Contracting Officer's Representative (COR) and TSA Pre✓® Application Expansion program office to schedule and conduct interim deliverable discussions and review meetings as requested in the deliverables table or as necessary. At these meetings, the TSA program office shall review the in-progress deliverables to ensure that they meet the business requirements and provide clarification on issues raised by the Contractor. It is anticipated the interim deliverable discussions shall occur mainly for, but are not limited to, the planning, design and test preparation phases of the OTA as needed.

The Contractor shall coordinate with the TSA program office to schedule and conduct Critical Design Reviews (CDR) and Test Readiness Reviews (TRR) or Production Readiness Reviews (PRR) for initial and major development and deployment efforts as requested by the COR and program office. A CDR should be coordinated prior to development and a TRR and/or PRR should be scheduled prior to major testing or production implementation.

The general quality standards, set forth below, shall be applied to each Deliverable received from the Contractor under this contract:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables shall satisfy the requirements of the Government as specified herein.
- File Editing – All text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow DHS/TSA guidance. Where none exists, the Contractor shall coordinate approval of format with the COR.
- Timeliness – Deliverables shall be submitted on or before the due date/time specified.

Unless otherwise stated, and as applicable, the Government shall have 20 working days to review and provide comments to the Contractor prior to acceptance of all deliverables. The Contractor must then respond ten working days after receipt of Government comments. All deliverables shall be submitted electronically, to the COR, CO and PM for review and approval. For presentations and/or briefings, the Contractor shall use MS Office Suite or other requested mediums compatible with the TSA program environment.

Deliverables related to procedures, management plans, training plans, security plans and IT deliverables shall be considered living documents that shall be updated as applicable by the Contractor.

#	Deliverable	Submitted Date	Review Date	Implement Date	Deliverable Recipient (include contact information)	Deliverable Format	Reference (specify Contract Data Requirements List (CDRL), attachments, etc.)
A001	.GOV Domain Name	At Time of Proposal	Within 5 calendar days	At OTA Award	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.14.5
A002	Monthly Report	On the 10th of the following month	Within 5 calendar days	N/A	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.13
A003	Privacy Notice	At OTA Award	Within 5 calendar days	At OTA Award	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.1

A004	Terms and Conditions Notice	At OTA Award	Within 5 calendar days	At OTA Award	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.8
A005	Concept of Operations	At OTA Award and anytime changes are either proposed by the Contractor or required by TSA	Within 5 calendar days	At OTA Award	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.1, 4.2, 4.3, 4.4, 4.5, 4.8
A006	Marketing Plan and Materials	At OTA Award and anytime changes are either proposed by the Contractor or required by TSA	Within 5 calendar days	At OTA Award	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.7

A007	Communications Management Plan	At OTA Award and anytime changes are either proposed by the Contractor or required by TSA	Within 5 calendar days	At OTA Award	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.6
A008	Quality Control Plan (QCP)	45 days after OTA award and anytime changes are either proposed by the Contractor or required by TSA	Within 10 business days	Within 5 calendar days after receipt	CO, COR and PM	Microsoft Office Documents e.g., Word,	Section 4.10
A009	Data Quality Control Plan	For Review and Approval prior to deployment/ implementation	Within 10 business days	Within 5 business days after receipt	CO, COR and PM	Microsoft Office Documents e.g., Word,	Section 4.10.2

A010	Security Authorization Package (as defined in Section 4.14.3 – D5)	For Review and Approval prior to deployment/ implementation	Within 5 business days	Within 5 business days after receipt	CO, COR and PM	Microsoft Office Document e.g., Word or Excel	Section 4.14.3
A011	System Design/Documentation	For Review and Approval prior to deployment/ implementation	Within 5 business days	Within 5 business days after receipt	CO, COTR and PM	Microsoft Office Document e.g., Word or Excel	Section 4.1.1, 4.1.2, 4.1.3
A012	Fingerprint Collection and Transmission Procedures	60 days after OTA award and anytime changes are either proposed by the Contractor or required by TSA	Within 10 business days	1st Enrollment	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.1.3.1

A013	Fee Collection and Submission Procedures	60 days after OTA award	Within 10 business days	1st Enrollment	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.4.2
A014	Personnel Training Plan	60 days after OTA award	Within 10 business days	N/A	CO, COR and PM	Microsoft Office Document e.g., Word or Excel	Section 4.1.4.1
A015	Customer Service Plan and Standard Operating Procedures (to include scripts)	60 days after OTA award and anytime changes are either proposed by the Contractor or required by TSA	Within 10 business days	N/A	CO, COR and PM	Microsoft Office Document e.g., Word or Excel	Section 4.5

A016	Ad-Hoc Reports	As Required	Within 5 calendar days	N/A	CO, COR and PM	Microsoft Office Document, e.g., Word or Excel	Section 4.13.2

Special Delivery Instructions:

Performance/ Delivery Period:
TSA reserves the right to award OTAs with a total period of performance not to exceed ten (10) years in duration.

Place/ Location of Performance/ Delivery:
Contractors that receive OTAs will be able to enroll and pre-screen applicants for TSA Pre✓® nationwide upon successful completion of all performance testing. Contractors must demonstrate the capability for applicants to begin the application process for TSA Pre✓® online through a secure, fully-encrypted, website and then direct applicants to complete the process at a physical location which is equipped for applicants to provide original or certified copies of TSA-approved identity documents.

In addition, physical locations must be staffed and equipped to capture biometrics from applicants. This includes manned locations to supervise the submission of biometrics and documents, deter fraud, and prevent physical hacks into the kiosks or attaching skimmers. Physical locations may be deployed onsite at airport locations and at offsite locations which demonstrate mass customer interface potential and favorable market penetration capabilities.

Due to the dynamic and changing cyber security environment, and because these systems will be targets of cyber criminals and other cyber threats, an ongoing red-teaming process will be used to identify and to remedy and existing database and transmission vulnerabilities.

4.16 Personnel Security

All contractors seeking to work on TSA unclassified contracts will be required to undergo vetting through the TSA Personnel Security Section (PERSEC) if one or more of the following access requirements exits:

1. Unescorted access to TSA facilities (includes leased spaces).
2. Access to DHS/TSA IT systems (to include TSA e-mail accounts) or assist in the development, operation, management or maintenance of DHS/TSA IT systems.
3. Access to TSA Sensitive but Unclassified (SBU) information which may include Sensitive Security Information (SSI).

United States citizenship is required to have access to DHS/TSA IT systems (to include TSA e-mail accounts) or assist in the development, operation, management or maintenance of DHS/TSA IT systems.

All contractors seeking to work on TSA unclassified contracts undergo the following three phased vetting process:

Phase 1: Preliminary Background Check: a review of an individual's consumer credit report, criminal history records, and submitted security forms to determine, to the extent possible, if the individual has bad debt and/or criminal offenses and/or falsification issues that would prohibit employment as a TSA contractor. A favorable Preliminary Background Check is not a final fitness determination; rather, it is a preliminary review of the commercial data that allows the individual to commence contract employment prior to the required background investigation being completed. When an individual is deemed eligible to commence employment on a TSA contract, TSA Personnel Security will notify the appropriate Contracting Officer's Technical Representative (COR) of the favorable determination. Similar notifications will be sent when an individual has not passed the preliminary background check and has been deemed ineligible to commence contract employment. In these situations, the contractor applicant is sent a letter which identifies the specific issues and provides a reconsideration response option with instructions regarding how to reply to PERSEC.

Phase 2: Background Investigation: Once the individual commences work on a TSA contract, TSA Personnel Security will process all submitted security forms to determine whether the contractor has previously been the subject of a federal background investigation sufficient in scope to meet TSA minimum investigative requirements. Contractors who have a federal investigation sufficient in scope will immediately be processed for final fitness adjudication. Those contractors who do not have a previous federal background investigation sufficient in scope will be scheduled for the appropriate level background investigation through the submission of their security forms to the Office of Personnel Management (OPM).

Phase 3: Final Suitability Adjudication: TSA Personnel Security will complete the final fitness adjudication after receipt and review of the completed OPM background investigation. The final fitness adjudication is an assessment made by TSA Personnel Security to determine whether there is reasonable expectation that the continued

employment of the TSA contractor will or will not protect or promote the efficiency of the agency. An unfavorable final fitness determination will result in a notification to the COR that the contractor has been deemed unfit for continued employment and that he/she shall be removed from the TSA contract.

Security Training Requirements
Contractor shall ensure all staff supporting this effort complete TSA provided IT Security Awareness Training within 60 days of assignment to the OTA and at a minimum annually thereafter. The Contractor shall ensure all staff supporting this effort completes other security training as requested by TSA such as handling of SSI and PII. The Contractor shall provide TSA training completion documentation upon request.

Any additional education and/or training provided by the Contractor to its employees shall meet standards established by the National Institute of Standards and Technology (NIST) and DHS policy.

Special Requirements:
Pre-Employment Security Screening of Contractor Employees

The Contractor shall ensure that each employee meets the Standard Operating Procedures for Enter-On-Duty Suitability Determination as determined by the Office of Personnel Security. TSA Standard Operating Procedures for Enter-On-Duty Suitability Processing for Contractors and Management Directive 2800.71 shall apply and be provided to the Contractor as reference. In addition, all trusted agents conducting enrollment activities are required to complete a full TSA STA) prior to conducting enrollment activities.

Key Personnel Requirements

For the purposes of this OTA contract, the Contractor's Program Manager, Customer Service Manager, Technical Architect, Personnel Security Manager, and Information Systems Security Officer (ISSO) shall be considered key personnel. The Contractor shall submit a resume to the CO and COR for the approval prior to bringing on board a new program manager or operations manager.

Changes to Key Personnel must be submitted to and approved by TSA. Key personnel must remain assigned to the OTA by the Contractor on a full or part-time basis (depending on the level of effort) for the full period of performance of the contract barring circumstances outside the control of the Contractor (e.g. death, resignation, disability, etc.) or as otherwise approved by the CO due to a change of duties, promotion, etc.