First Advantage

TSA PRECHECK SERVICES ADDITIONAL TERMS AND CONDITIONS

These TSA PreCheck Services Additional Terms and Conditions are applicable to Providers performing TSA Precheck Services. Provider is also referred to herein as "Seller."

Provider understands that Telos ID has entered into an Other Transaction Agreement ("OTA") Contract No. 70T020209NTOIA011 with the Transportation Security Administration ("TSA" or "Customer") for the purposes of implementing TSA's PreCheck® Biometric Expansion Program ("TSA PreCheck Services") (hereinafter referred to as "Prime Contract"); and FAESC has entered into a contract with Telos ID to provide TSA Precheck Services. FAESC is engaging Provider as a subcontractor to provide TSA Precheck Services ("Subcontract").

1. **Personnel**. Seller's personnel performing the Services shall be U.S. citizens and must pass various background checks before performing services. For Services performed at the Seller's facility, the normal working hours of the Seller's facility will be observed. The Seller shall be responsible for selecting, screening and supervising Seller personnel who are qualified and possess the skill level of expertise to successfully render the services. To the extent permitted by law, all Seller personnel shall be subject to a diligent background investigation conducted by Seller and/or a third-party company specializing in background investigations. All such background investigations shall be conducted in full compliance with all laws in the applicable jurisdiction. Seller shall not permit any personnel to have access to the equipment or to provide services or work under this Agreement unless they have passed the background investigations under the specifications set forth herein. In the event the background screening requires the inclusion of specific criteria in the background investigation, including a seven (7) year "look-back" period and drug testing, Seller shall comply with all specific criteria which shall be communicated to Seller in writing or which is required in the Fingerprint Capture Service Center Agreement.

2. **Equal Employment Opportunity Clause.** The Equal Employment Opportunity Clause required under Executive Order 11246, and the employee notice clause pertaining to employee rights under the National Labor Relations Act, set forth in 29 CFR Part 471 Appendix A to Subpart A, are incorporated by reference in this Agreement. By accepting this agreement, Seller additionally certifies that, to the extent applicable, **Seller shall abide by the requirements of 41 CFR §§ 60-1.4(a), 60-300.5(a) and 60-741.5(a). These regulations prohibit discrimination against qualified individuals based on their status as protected veterans or individuals with disabilities, and prohibit discrimination against all individuals based on their race, color, religion, sex, or national origin. Moreover, these regulations require that covered prime contractors and subcontractors take affirmative action to employ and advance in employment individuals without regard to race, color, religion, sex, national origin, protected veteran status or disability."**, that it complies with the authorities cited above, and that it does not maintain segregated facilities or permit its employees to perform services at locations where segregated facilities are maintained, as required by 41 CFR 60-1.8.

3. **No Subcontracting**. The Seller shall not subcontract any part of the Services to be performed.

4. **Status Reporting and Reviews**. If requested, the Seller shall provide status and relevant accounting reports on a weekly basis (or at a frequency as otherwise directed by FAESC) and support FAESC, program reviews as required by Telos ID and/or the TSA.

5. **Information Security.** Seller shall not process, store, or transmit data, or allow data to be accessed outside of the United States. Seller shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve and assure the confidentiality, integrity, and availability of the data. Seller shall be fully responsible for the acts and omissions of its personnel. During the term of this Agreement, FAESC, Telos, or its designated authorized representative, will have the right to reasonably inspect and audit Seller's records for the purpose of confirming compliance with this Information Security clause. Any such inspection and audit will be conducted no more than once annually during regular business hours and in a manner that minimizes interference with Seller's normal business activities.

6. **Data Breach Notification.** Upon the discovery by the Seller of a breach of security that results in the unauthorized release, disclosure, or acquisition of confidential information, biometric data or personal information, the Seller shall provide notice to FAESC as soon as reasonably possible (the "Initial Notice"). The Initial Notice shall be delivered to FAESC by electronic mail to the contact currently on file and shall include the following information, to the extent known at the time of notification: i) a description of the nature of the breach; ii) the name and contact details of the data protection officer or other point of contact from whom more information can be obtained; iii) a description of the likely consequences of the data breach; and iv) a description of the measures taken or proposed to be taken by the Seller to address the data breach.

7. **Loss/Damage to Property**. The Seller assumes full responsibility, and shall compensate FAESC for any and all losses or damage of whatsoever kind and nature to any and all Telos ID or Government property, including any equipment, supplies, accessories or parts furnished while in custody and care for storage, repairs, or services to be performed under the terms of this Subcontract resulting, in whole or in part from the acts or omissions of Seller; provided that Telos ID or the Government seeks reimbursement or compensation from FAESC for such losses or damage to such property.

8. **Rights in Data and Works**. The following rights in data and works will apply to the Services provided by Seller under this Subcontract:
   a. Telos ID reserves all rights in the intellectual property, patents, patents pending, copyrights, trade secrets, trade names, trademarks, service marks and to any other commercial symbols which it now owns or may hereafter acquire, develop or use. No license to the Seller, under any trademark, patent, copyright, or other intellectual property right which is now, or may be, owned by Telos ID shall be granted under this Subcontract.
   b. Any and all inventions, discoveries, improvements, or creations (collectively "Creations") which Seller has conceived or made or may conceive or make during the period of this Subcontract directly and solely connected with the provision of Services to Telos shall be the sole and exclusive property of Telos ID. Although the parties agree that no "works made for hire" are contemplated under this Agreement, to the extent applicable, Seller agrees that all copyrightable works created by Seller hereunder or in connection with the Services are "works made for hire". Seller hereby assigns all proprietary rights, including copyright, in these

works to Telos ID without further compensation. Seller further agrees to (i) disclose promptly to Telos ID all such Creations which Seller has made or may make solely, jointly, or commonly with others, (ii) assign all such Creations to Telos ID, and (iii) execute and sign any and all applications, assignments, or other instruments which Telos ID may deem necessary in order to enable Telos ID, at its expense, to apply for, prosecute, and obtain copyrights, patents or other proprietary rights in the United States and foreign countries or in order to transfer to Telos all right, title, and interest in said Creations.

c. The parties acknowledge that Telos ID, on the one hand, and Seller, on the other, may have pre-existing professional knowledge, know how, materials, methods, and/or techniques, developed by, and/or in its possession, including those which may have been copyrighted and/or patented by such party or constitute a trade secret, prior to the effective date of this Subcontract (such party's "Intellectual Capital") which may be accessed, modified or enhanced in the provision of Services hereunder. The parties agree that, except as specifically provided in this Subcontract or any Proposal, the other party will not acquire title or interest to any of the other party's Intellectual Capital. Nothing in this clause shall be construed or interpreted as imposing any restriction on Telos ID's or Seller's disclosure or use of any general learning, skills or know–how, commonly referred to as "general expertise," acquired by such party and their personnel in connection with the Services provided under this Subcontract if such disclosure or use would be regarded by a person of ordinary skill in the relevant technology as not constituting a disclosure or use of the other party's confidential information.

9. **Warranty.** The Seller warrants that the Services shall be provided by qualified and competent personnel; that such personnel have the necessary education, training and/or experience to meet the requirements, as delineated herein and perform the Services satisfactorily; that the Services shall be in accordance with any specifications, descriptions, and/or Statement of Work or incorporated herein, and that the Services shall be performed in a professional and workmanlike manner and shall be fit for the intended purpose and use if made known to the Seller. The Seller further warrants that it shall fully comply with city, state, and federal laws, regulations, and/or ordinances pertinent to performance of the Services, including that the Seller's personnel shall observe all safety and security rules and regulations for the facility where the Services are performed. If the Services are not as warranted, FAESC shall have the right, notwithstanding any payments for or inspection or acceptance of the Services, to require correction or replacement. Any Services requiring correction or replacement shall be corrected or replaced by and at the expense of the Seller, promptly after written notice from FAESC. If the Seller fails to correct or replace the Services as required, FAESC may either perform the Services itself or contract with others to obtain such services or goods, in which event any increased project costs shall be immediately owed by the Seller to FAESC, or FAESC may terminate the Subcontract for default, provided that the stated remedies of FAESC shall not be deemed exclusive, but shall be in addition to any other remedies provided elsewhere in this Subcontract or available to it by law. The warranties of the Seller as set forth herein shall survive inspection, acceptance and payment hereunder.

10. **Termination.** Upon termination of this Subcontract the Seller shall promptly return all equipment provided for the TSA PreCheck Services including that belonging to FAESC, Telos (and the Government's, as applicable) data, programs, and other materials held by it in connection with the performance of this Subcontract. FAESC may terminate this Subcontract for convenience. Either party may immediately terminate this Subcontract if the other party appears on the "Lists of Parties Excluded from Federal Procurement or Non-procurement Programs" or any superseding document issued by the U.S. General Services Administration Office of Acquisition Policy. All terms of this Subcontract are binding up to the time of termination. Moreover, the parties' obligations and/or rights under the Subcontract, specifically the obligations and/or rights related to records, inspection and acceptance, warranty, confidential and proprietary information, rights in data and works, non-solicitation/non-hiring, indemnification, and limitation of liability shall survive expiration or termination of this Subcontract. The rights and remedies of FAESC are in addition to any other rights and remedies provided by law or under this Subcontract.

11. **Non-Interference/Non-Solicitation.** During the term of the Subcontract Seller will have access to valuable Confidential Information and trade secrets of FAESC and/or Telos in the course of its performance of the TSA PreCheck Services. Seller agrees to provide the services contracted under the auspices of this Subcontract and any resulting purchase order exclusively through Telos and will not provide the same or similar services using Telos' equipment or authority for the TSA PreCheck Enrollment Program through a third-party, or divert or attempt to divert any enrollment services or competitive business from Telos during the term of this Subcontract and for a period of one year after following any expiration or termination of this Subcontract. The Parties agree that for the duration of the Subcontract and for one (1) year after the date of termination or expiration of the Subcontract, neither party will directly or indirectly recruit, solicit or hire as an employee or independent contractor any person employed by the other as an employee without the other party's prior written consent. Notwithstanding the foregoing, neither party shall be precluded from hiring any such employee who initiates discussions regarding such employment without any direct solicitation by the hiring party or who responds to any public advertisement placed in any medium by the hiring party.

12. **Insurance.** During the entire performance period of this Subcontract, Seller shall, at its own expense, provide and maintain insurance coverage for at least the kinds and minimum amounts set forth below. All required insurance is to be placed with insurers with a current A.M. Best Financial Strength rating of no less than "A-" and a Financial Size Category (FSC) of "VII", unless otherwise approved, in writing, by the Telos ID Contracts Representative. Telos ID reserves the right to require any other insurance coverage which Telos ID considers reasonably necessary or appropriate under the circumstances of the applicable Purchase Order, which requirement for insurance shall be communicated to the Seller prior to or concurrently with the applicable Purchase Order for which such coverage is required.

    a. Workers' Compensation Insurance in accordance with the amounts specified by the laws of the states in which the Services are to be performed under this Subcontract.

    b. Employer's Liability Insurance with minimum limits of $500,000 per accident for bodily injury by accident, $500,000 policy limit by disease, and $500,000 per employee for bodily injury by disease.

    c. Commercial General Liability Insurance, on an occurrence form and to include Premises and Operations, Products/Competed Operations, Contractual Liability, including the tort liability of another assumed in a business contract, personal injury and advertising

injury, Broad Form Property Damage and Independent Contractors Liability, in the minimum amount of $1,000,000 per occurrence (combined single limit for bodily injury and/or property damage), $1,000,000 for Personal Injury Liability, $1,000,000 Aggregate for Products and Completed Operations, and $2,000,000 General Aggregate. The General Aggregate should apply per Project. Products and Completed Operations coverage shall be maintained for two (2) years after final completion of the Project including coverage for the Additional Insureds. If work called for in this contract is performed outside of the United States worldwide coverage and jurisdiction shall apply. The coverage afforded FAESC will be primary and non-contributory over any other insurance maintained by FAESC. Notice of policy cancellation shall be provided in accordance with policy provisions and Seller will advise FAESC of any material change in coverage affecting the contract.

d. Umbrella or Excess Liability Coverage in the amount of $5,000,000 per occurrence and aggregate to provide insurance in excess of Employer's Liability, Commercial General Liability and Automobile Liability Policies.

e. All-Risk Property Insurance, if applicable, to adequately cover the replacement cost for any property and/or equipment provided to Seller in Seller's care, custody, and control.

f. Professional Liability Insurance, providing coverage for claims arising out of the performance of professional services, resulting from any error, omission or negligent act of the Seller, in an amount no less than $1,000,000 per occurrence and aggregate.

g. To the extent that the Seller provides software hardware, software or system development, consulting services, or internet/application services to FAESC, the following shall also apply:

i. Seller shall purchase the following: Technology/Professional Liability, Media Liability and Network Security/Privacy ("Cyber") Liability Insurance covering acts, errors, omissions, breach of contract, and violation of any consumer privacy protection laws arising out of Seller's operations or services with a limit of $2,000,000 per claim and in the aggregate. Such coverage shall include but not be limited to, third party and first party coverage for loss or disclosure of any data, including personally identifiable information and payment card information, network security failure, violation of any consumer privacy protection laws, unauthorized access and/or use or other intrusions, infringement of any intellectual property rights (except patent), unintentional breach of contract, negligence or breach of duty to use reasonable care, breach of any duty of confidentiality, invasion of privacy, or violations of any other legal protections for personal information, defamation, libel, slander, commercial disparagement, negligent transmission of computer virus, or use of computer networks in connection with denial of service attacks. Such coverage shall include contractual privacy coverage for data breach response and crisis. management costs that would be incurred by Seller on behalf of FAESC in the event of a data breach including legal and forensic expenses, notification costs, credit monitoring costs, and costs to operate a call center. Seller shall maintain Cyber Liability Insurance coverage in force during the term of this Subcontract and for an extended reporting period of not less than 3 years after.

h. Prior to commencement of work hereunder, the Seller shall furnish FAESC with a certificate of insurance providing evidence of the above-required insurance. The certificate must include the contract and/or purchase order number and includes the following:

i. General liability and auto policies (except for the Workers' Compensation and Employer's Liability insurance policies) shall include FAESC, its corporate affiliates, subsidiaries, officers, directors and any employee or agents as Additional Insureds and shall stipulate that the insurance afforded to such Additional Insureds shall apply as primary insurance. Coverage afforded the additional insured under the general liability policy will apply to completed operations coverage for a period of two years after completion of the work. General liability, auto, and workers compensation/employers liability policies shall contain waivers of insurer's subrogation rights in favor of FAESC.

ii. FAESC shall be named as Loss Payee with respect to All-Risk Property if Seller has care, custody and control of FAESC's (and/or FAESC's customer's) property and/or equipment.

13. **Records.** The Seller shall maintain sufficient records concerning its performance to permit verification through normal audit procedures of costs invoiced by the Seller in the performance of the TSA PreCheck Services. The Seller agrees that its books and records, or such part thereof as may be engaged in the performance of this Subcontract shall at all reasonable times be subject to inspection and audit by any authorized representative of FAESC, Telos ID and/or the Government. This right shall survive acceptance and final payment on this Subcontract for a period of five (5) years.

14. **Export Control and Foreign Corrupt Practices Act.** In the performance of this agreement, the Provider shall comply with all applicable US laws and regulations concerning export controls, boycotts and corrupt practices, incl., but not limited to, the Arms Export Control Act, the Export Administration Act of 1979, the Export Administration Regulations ("EAR"), the International Traffic in Arms Regulations ("ITAR"), and U.S. sanctions and embargoes administered by the U.S. Department of Treasury, Office of Foreign Assets Control ("OFAC"). The ITAR, EAR, and U.S. sanctions and embargoes may require prior written authorization from the U.S. government for export, re-export, and transfer of goods, services and data. The Provider shall consult with the Department of State regarding any questions relating to the compliance with ITAR and with the Department of Commerce regarding any questions relating to compliance with the EAR.

The Provider understands and acknowledges that Telos ID is subject to the provisions of the U.S. Foreign Corrupt Practices Act ("FCPA"), which makes it unlawful to offer, pay, promise or authorize to pay any money, gift or anything of value, incl., but not limited to bribes, entertainment, kickbacks or any benefit, directly or indirectly, to any foreign official. The Provider agrees to not engage in any activity, whether directly or indirectly, that will violate any of the requirements of the FCPA, and agrees to promptly notify FAESC of any information related to this agreement or Telos ID's products, services, or data indicating a potential conflict with the requirements of the FCPA. The term "foreign official" shall include, but is not limited to, any officer, employee, or agent of a government, state-owned corporate entity, public international organization, political party, candidate for public office, and any department, agency, or instrumentality thereof.

15. **Non-Disparagement**. Seller agrees that Seller, its agents and representatives shall not make or publish, directly or indirectly, disparaging comments concerning FAESC or Telos ID, whether or not slanderous or libelous, to any third party, including but not limited to any third party who is receiving the benefit of the Seller's Services, (hereinafter referred to as "Third Party"). Seller also agrees not to make or publish, directly or indirectly, disparaging comments concerning any employee, agent or representative of Telos ID, including disparaging or negative comments, either formally or informally, to a Third Party regarding performance of duties, ability, experience or qualifications.

16. **Independent Contractor**. Seller is an independent contractor and neither party's employees will be considered employees of the other party for any purpose. Further, Seller, and its employees, shall in no sense be considered employees or agents of FAESC or Telos ID nor shall they be entitled or eligible to participate in any benefits or privileges given or extended by FAESC or Telos ID to its employees, or be deemed an employee of FAESC or Telos for purposes of federal or state withholding taxes, disability, FICA taxes, unemployment compensation, Worker's Compensation or Employer's Liability Insurance, and any other contributions due on behalf of itself to its employees. Employees provided by Seller will be bona fide employees of Seller. Seller assumes full responsibility for actions of its personnel while performing work. Seller and its employees shall indemnify and hold FAESC and/or Telos ID harmless in the event Seller does not properly conform to this Subcontract pertaining to the withholding of FICA, disability, and federal, state and municipal withholding taxes. This Subcontract does not create a joint venture or partnership, and neither party has the authority to bind the other to any third party. Additionally, Seller will represent itself as an independent entity, and not as an affiliate of the Transportation Security Administration or Department of Homeland Security.

17. Press Releases. Any news releases, public announcements, advertisements, web postings, social media postings, or publicity released by the Seller concerning this Subcontract, including any Purchase Order, will be subject to prior written approval of FAESC.

EXHIBIT A

TO THE

TSA PRECHECK SERVICES ADDITIONAL TERMS AND CONDITIONS

PROGRAM DESCRIPTION

Agreement Program Scope: TSA requests ready-to-market solutions to add private sector application capabilities for the TSA PreCheck® Application Program to increase the methods and capabilities available for the public to enroll in the TSA PreCheck® program, as required by the TSA Modernization Act of 2018, Section 1937(d), H.R. 302.

Companies that want to propose a private sector application capability must provide the capability to enroll and vet a large population of applicants through the collection of biometric data.

1. Background

The TSA PreCheck® Application Program is a voluntary passenger prescreening initiative that determines whether passengers are low risk and thus eligible to receive expedited screening at participating U.S. airport security checkpoints. The TSA PreCheck® Application Program is one of multiple trusted traveler programs and methods by which a passenger may be determined eligible for TSA PreCheck® screening at participating airport checkpoints. As part of TSA's broader TSA PreCheck® screening, travelers in the TSA PreCheck® Application Program are allowed 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 airport screening lanes. Travelers who choose not to enroll, or are determined ineligible for TSA PreCheck® , are processed through standard TSA security screening protocols.

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

Currently, there are several ways for individuals to enroll for TSA PreCheck® . These channels include the current Department of Homeland Security Trusted Traveler Programs, including TSA PreCheck® 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 PreCheck® .

TSA PreCheck® Application Expansion Approach:

The TSA PreCheck® Expansion initiative will expand enrollment into TSA PreCheck® by companies that receive Other Transactional Agreements (OTAs) from TSA. Companies must have a start-to-finish secure online or mobile enrollment capability. For the purposes of this solicitation, online enrollment capability is described as the ability to enroll via a web portal or a mobile application; mobile enrollment capability is described as the ability to enroll with equipment that is portable and can be moved to meet customer demand and location preferences (e.g., tablets, kiosks, etc.). After an applicant completes the enrollment process, the OTA Entity shall vet the applicant by means of the applicant's biometric data by conducting a criminal history records check through the Federal Bureau of Investigation (FBI) and submit any resulting criminal history information (CHRI) to TSA.

TSA will then determine applicant eligibility through a comprehensive Risk Assessment. This Risk Assessment is sometimes referenced as a Security Threat Assessment (STA), which is a more general term applicable to TSA's transportation sector vetting programs (including the TSA PreCheck® Application Program). TSA's STA process includes a review of the criminal history information, verification of U.S. Citizenship and Lawful Permanent Resident (LPR) status, and terrorism-related database checks.

<u>Identity Assurance/Verification</u>

Any solution used for identity assurance/verification must receive TSA approval.

With regard to the Program, the relevant legal, regulatory, policy and security documents are cited below. The OTA Entity shall adhere to the latest version of the documentation referenced below or otherwise as cited elsewhere in the Statement of Work that has been specifically delineated and assigned via awarded purchase order(s). If the

- Public Law 107-347, Federal Information Security Management Act (FISMA) of 2002.
- Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources.
- Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d)
- The Privacy Act of 1974 (5 U.S.C. § 552a)
- DHS Management Directive 4300A - Sensitive Systems Policy: Information Technology Security Program
- DHS Management Directive 4300B - National Security Systems Policy Publication: Information Technology Security Program
- DHS Management Directive 11042: Safeguarding Sensitive but Unclassified (For Official Use Only) Information

- FBI Electronic Biometric Transmission Specification
- FIPS Publication 201-1 Personal Identity Verification (PIV) of Federal Employees and Offerors (March 14, 2006)
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 140-2, Security Requirements for Cryptographic Modules
- ICAO document 9303 titled “Machine Readable Travel Documents”, Seventh Edition, dated 2015
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Technology Systems
- NIST Special Publication 800-63, Electronic Authentication Guideline
- NIST Special Publication 800-88, Guidelines for Media Sanitization
- TSA Management Directive 1400.3 TSA Information Security Policy
- TSA Management Directive 2800.71 Pre-Employment Investigative Standards for TSA Non-Screener Employees and Offerors
- TSA Management Directive 3700.4 Handling Sensitive Personally Identifiable Information (SPII)

EXHIBIT B TO THE

TSA PRECHECK SERVICES ADDITIONAL TERMS AND CONDITIONS

PRIME CONTRACT SPECIFIC TERMS AND CONDITIONS

Seller shall comply with the following clauses extracted and flowed down from Telos ID's Prime Contract, unless the context of the clause requires otherwise, the term "Contractor" shall mean "Seller", the term "Contract" shall mean the "Purchase Order", and the terms "Government" and equivalent phrases shall mean "Telos ID". The term "Contracting Officer" shall mean the "Telos ID Contracts Representative". It is intended that the reference clauses shall apply to Seller in such manner as is necessary to reflect the position to Telos ID and to Telos ID's Government customer, and to enable Telos ID to meet its obligations under its Prime Contract.

ARTICLE XVIII – PROTECTION OF INFORMATION/EMPLOYEE ACCESS/

SAFEGUARDING SENSITIVE INFORMATION

Applicability. This article applies to Telos ID subcontractors, and their Entity employees (hereafter referred to collectively as "OTA Entity"). The OTA Entity shall insert the substance of this article in all subcontracts.

Definitions

(a) "Sensitive Information", as used in this article, 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) "Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

(2) PII is a subset of sensitive information. Examples of PII include, but are not limited to: 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), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, 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.

(3) 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);

(4) 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);

(5) 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

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

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, OTA Entity system, or sensitive information.

Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)

(2) Date of birth (month, day, and year)

(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(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.

1. PROTECTION OF INFORMATION

The OTA Entity agrees that they shall take appropriate measures to protect proprietary, privileged, or otherwise confidential information that may come into their possession as a result of this Agreement.

A. Records and Release of Information

Pursuant to 49 U.S.C. § 114(r), Sensitive Security Information and Nondisclosure of Security Activities, Sensitive Security Information (SSI) is a category of sensitive but unclassified (SBU) information that must be protected because it is information that, if publicly released, would be detrimental to the security of transportation. Under 49 Code of Federal Regulations Part 1520.5(a), the SSI Regulation also provides additional reasons for protecting information as SSI beyond the condition that the release of the information would be detrimental to the security of transportation. SSI may not be disclosed except in accordance with the provisions of that rule.

Title 49 of the Code of Federal Regulations, Part 1520 defines the scope, categorization, handling requirements and disposition of information deemed SSI is the 49 C.F.R. Part 1520 (http://ecfr.gpoaccess.gov/). All members of OTA Entity assigned to work under this Agreement are subject to the provisions of 49 CFR Part 1520, Protection of Sensitive Security Information, and shall safeguard and handle any SSI in accordance with the policies and procedures outlined in 49 C.F.R. Part 1520, as well as the DHS and TSA policies and procedures for handling and safeguarding SSI. All members of OTA Entity assigned to work under this Agreement must complete the TSA-mandated SSI Awareness Training course prior to accessing SSI, and on an annual basis for the duration of the OTA or for the duration of the requester's need for access to SSI, whichever is later. The OTA Entity shall place this requirement in all contracts, sub-contracts, joint venture agreements, and teaming agreements related to the performance of this agreement. For purposes of this Agreement, the OTA Entity would fall under the provision of 49 CFR § 1520.7(k): Each person employed by, contracted to, or acting for a covered person, including a grantee of DHS or DOT, and including a person formerly in such position.

Non-Disclosure Agreements (NDAs). Buyer will provide the non-disclosure form (DHS Form 11000-6), as necessary, to the OA Entity when circumstances warrant. NDAs are required to be signed by all OTA Entity personnel when access to SSI is necessary for performance of the agreement. By signing the NDA, the recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information.

Breach. In accordance with 49 C.F.R. Part 1520.9(c), the OTA Entity agrees that in the event of any actual or suspected breach of SSI (i.e., loss of control, compromise, unauthorized disclosure, access for an unauthorized purpose, or other unauthorized access, whether physical or electronic), the OTA Entity shall immediately, and in no event later than one hour of discovery, report the breach to the Telos ID program manager and contracts representative identified in this Agreement.

I. Background. OTA Entity members assigned to work under this Agreement must obtain specific authorization in order to obtain SSI. SSI will not be available or otherwise provided or disclosed to any person not specifically authorized to receive it. As part of the TSA program relevant to this Agreement, , SSI may only be accessed by individuals which have successfully passed a Security Threat Assessment. This assessment may include a criminal history records check (CHRC) and/or a check against terrorism databases.

II. Information Requirements. Consistent with the criteria release described above, the Agreement Holder shall provide the appropriate information to the Telos ID Program Manager ("Telos ID PM") as needed. Note that this requirement applies likewise to all contracts, sub-contracts, joint venture agreements, and teaming agreements related to the performance of this agreement. This information will be handled in accordance with the applicable Privacy Act system of records notice (SORN), Transportation Security Threat Assessment System (T-STAS) noted below.

1. The Agreement Holder shall provide the following information for all employees who require access to SSI in a single password protected Microsoft Excel spreadsheet emailed to the Telos ID PM. The password for the password protected spreadsheet shall be sent to the COR in a separate email, at the same time.

   - Employee Full Name
   - Employee Gender: (i.e., Male or Female)

- Employee Birth Date
- Employee Citizenship
- Social Security Number (for U.S. Citizens and Legal Permanent Residents only)
- Known Traveler Number (KTN), if available

III. Privacy Act Statement. TSA will use the information provided to conduct a security threat assessment on individuals who seek access to Sensitive Security Information (SSI). The information will be shared within DHS with personnel who need the information to perform their official duties. Additionally, DHS may share the information with law enforcement, intelligence, or other government agencies as necessary to identify and respond to potential or actual threats to transportation security in accordance with the routine uses identified in the applicable Privacy Act system of records notice (SORN), DHS/TSA 002, Transportation Security Threat Assessment System (T-STAS). This SORN was last published in the Federal Register on August 11, 2014 and can be found at 79 FR 46862-46866. Authority: 49 USC 114. Furnishing this information is voluntary. However, failure to furnish the requested information may delay or prevent the completion of your security threat assessment, without which you may not be granted access to the SSI.

IV. Notification of Assessment. Individuals who receive a successful Security Threat Assessment will be eligible to receive SSI. If it is determined that covered individuals are not eligible to receive access to particular SSI based on the threat assessment, the TSA Contacting Officer or COR will provide the appropriate point of contact with notification that the individual does not qualify to receive SSI. Appeal of the determination will not be permitted due to the time sensitive nature of the acquisition process; however, the potential OTA Entity may be entitled to nominate another individual to receive SSI access if the Telos PM approves the change. In the event that an individual is determined to be a security threat and the individual believes that the results of the screening are inaccurate, he or she may request access to their records by submitting a Privacy Act Request through TSA's Freedom of Information Act (FOIA) internet site at: https://www.tsa.gov/foia/requests.

B. Publicity and Dissemination of Agreement Information

The OTA Entity shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this Agreement without the prior written consent of the Telos ID PM and Telos ID Contracts Administrator. The Agreement holder shall submit any request for public release at least ten (10) business days in advance of the planned release. Under no circumstances shall the OTA Entity release any requested submittal prior to receiving appropriate approval.

Any material proposed to be published or distributed shall be submitted by Telos ID via email to the Contracting Officer. The Contracting Officer will follow the procedures in Management Directives 1700.3 and 1700.4. The Office of the Administrator retains the authority to deny publication authorization. Any conditions on the approval for release will be clearly described. Notice of disapproval will be accompanied by an explanation of the basis or bases for disapproval.

Any contact with or by a Media firm, or personnel related to this Agreement and in accordance with the terms of this Agreement shall be referred to the Telos ID PM.

2. OTA ENTITY EMPLOYEE ACCESS

OTA Entity 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 Telos ID PM. The OTA entity's employees shall be fingerprinted, or subject to other investigations as required. All OTA entity 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 under this Agreement unless this requirement is waived in writing by Telos ID.

Telos ID may require the OTA Entity 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.

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

The OTA Entity shall include the substance of this article in all subcontracts at any tier where the OTA's respective subcontractor may have access to Government facilities, sensitive information, or resources.

Before receiving access to IT resources under this Agreement, the individual must receive a security briefing which shall be facilitated through the direction of the Telos ID PM.

The OTA Entity shall have access only to those areas of DHS information technology resources explicitly stated in this contract or otherwise approved in writing as necessary for performance of the work under this Agreement. Any attempts by OTA Entity personnel to gain access to any information technology resources not expressly authorized by the Statement of Work, other terms and conditions in this Agreement, or as appropriately approved in writing, is strictly prohibited. In the event of violation of this provision, Telos ID will take appropriate actions

with regard to the Agreement and the individual(s) involved. OTA Entity access to DHS networks from a remote location is a temporary privilege for mutual convenience while the OTA Entity 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). OTA Entity access will be terminated for unauthorized use. The OTA Entity agrees to hold and save Telos ID 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.

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 Agreement, unless a waiver has been appropriately granted.

OTA Entity's shall identify 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 Telos PM and Telos Contracts Administrator.

3. SAFEGUARDING OF SENSITIVE INFORMATION

Authorities. The OTA Entity shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information

(2) DHS Sensitive Systems Policy Directive 4300A

(3) DHS 4300A Sensitive Systems Handbook and Attachments

(4) DHS Security Authorization Process Guide

(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information

(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program

(7) DHS Information Security Performance Plan (current fiscal year)

(8) DHS Privacy Incident Handling Guidance

(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html

(10) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html

(11) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

Handling of Sensitive Information. OTA Entity compliance with the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on OTA Entity personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information describes how OTA Entity must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The DHS Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook provide the policies and procedures on security for Information Technology (IT) resources. The DHS Handbook for Safeguarding Sensitive Personally Identifiable Information provides guidelines to help safeguard SPII in both paper and electronic form. DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(2) The OTA Entity shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the OTA Entity except as specified in the contract and as subsequently conveyed to OTA Entity on their program via awarded purchase order.

(3) All OTA Entity employees with access to sensitive information shall be required to execute DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA), as a condition of access to such information. The OTA Entity shall maintain signed copies of the NDA for all employees as a record of compliance. The OTA Entity shall provide copies of the signed NDA to the Telos ID PM or directly to Contracting Officer's Representative (COR) if permitted by Telos PM no later than two (2) days after execution of the form.

(4) The OTA Entity's invoicing, billing, and other recordkeeping systems maintained to support financial or other administrative functions shall not maintain SPII. It is acceptable to maintain in these systems the names, titles and contact information for the Government COR or other Government personnel associated with the administration of the contract, as needed.

(e) *Authority to Operate.* The OTA Entity shall not input, store, process, output, and/or transmit sensitive information within an OTA Entity IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The OTA Entity shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) *Complete the Security Authorization Process.* The SA process shall proceed according to the DHS Sensitive Systems Policy Directive 4300A (Version 11.0, April 30, 2014), or any successor publication, DHS 4300A Sensitive Systems Handbook (Version 9.1, July 24, 2012), or any successor publication, and the Security Authorization Process Guide including templates.

(i) *Security Authorization Process Documentation.* SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the OTA Entity shall submit a signed SA package, validated by an independent third party, to the Telos ID PM who will facilitate acceptance with the Customer. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. The Government's acceptance of the ATO does not alleviate the OTA Entity's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) *Independent Assessment.* OTA Entities shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations. TSA reserves the right to serve as the independent party to review and analyze security and privacy controls. The OTA Entity shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) *Support the completion of the Privacy Threshold Analysis (PTA) as needed.* As part of the SA process, the OTA Entity may be required to support the Customer in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a OTA Entity IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, appropriate determination shall be made as to whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The OTA Entity shall provide all support necessary to assist completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information about the use, access, storage, and maintenance of PII on the OTA Entity's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The OTA Entity is required to update its SA package as part of the ATO renewal process. The OTA Entity shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90-day review process is independent of the system production date and therefore it is important that the OTA Entity build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the OTA Entity environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The OTA Entity shall afford DHS, the Office of the Inspector General, and other Government organizations access to the OTA Entity's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The OTA Entity shall, through the proper communication channels, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, 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 Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All OTA Entity-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The plan is updated on an annual basis. The OTA Entity shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with FIPS 140-2 Security Requirements for Cryptographic Modules and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of OTA Entity systems from Government tools and infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, OTA Entity may be directed to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the OTA Entity IT system under this Agreement and associated program. Restricting access may include

disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* OTA Entity's operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. OTA Entity's shall provide the information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2014 DHS Information Security Performance Plan, or successor publication. The OTA Entity shall provide all information to fully satisfy Federal reporting requirements for OTA Entity systems.

Sensitive Information Incident Reporting Requirements.

(1) All known or suspected sensitive information incidents shall be reported immediately upon discovery to the Telos ID PM who will then report it to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with 4300A Sensitive Systems Handbook Incident Response and Reporting requirements. The OTA Entity shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the OTA Entity shall use FIPS 140-2 Security Requirements for Cryptographic Modules compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment. A sensitive information incident shall not, by itself, be interpreted as evidence that the OTA Entity has failed to provide adequate information security safeguards for sensitive information or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in 4300A Sensitive Systems Handbook Incident Response and Reporting, OTA Entity's shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Data Universal Numbering System (DUNS);

(ii) Contract numbers affected unless all contracts by the company are affected;

(iii) Facility CAGE code if the location of the event is different than the prime OTA Entity location;

(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, email);

(v) Contracting Officer POC (address, telephone, email);

(vi) Contract clearance level;

(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;

(viii) Government programs, platforms or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where sensitive information resided at the time of the incident, both at the OTA Entity and subcontractor level;

(xii) Description of the Government PII and/or SPII contained within the system;

(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and

(xiv) Any additional information relevant to the incident.

Sensitive Information Incident Response Requirements.

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy Officer.

(2) The OTA Entity shall provide full access and cooperation for all activities determined by the Government to be required to ensure an effective incident response, including providing all requested images, log files, and event information to facilitate rapid resolution of sensitive information incidents.

(3) Incident response activities determined to be required by the Government may include, but are not limited to, the following:

(i) Inspections,

(ii) Investigations,

(iii) Forensic reviews, and

(iv) Data analyses and processing.

(4) The Government, at its sole discretion, may obtain the assistance from other Federal agencies and/or third-party firms to aid in incident response activities.

Additional PII and/or SPII Notification Requirements.

(1) The OTA Entity shall have in place procedures and the capability to notify any individual whose PII resided in the OTA Entity IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise approved by the Contracting Officer. The method and content of any notification by the OTA Entity shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the DHS Privacy Incident Handling Guidance. The OTA Entity shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

(2) Subject to the requirements of applicable law, Government analysis of the incident and the terms of its instructions to the OTA Entity regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by the Government. Notification may require the OTA Entity's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;

(ii) A description of the types of PII and SPII involved;

(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;

(iv) Steps individuals may take to protect themselves;

(v) What the OTA Entity and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and

(vi) Information identifying who individuals may contact for additional information.

Credit Monitoring Requirements. In the event that a sensitive information incident involves PII or SPII, the OTA Entity may be required to, as directed by the Contracting Officer to the extent required by applicable law:

(1) Provide notification to affected individuals as described above; and/or

(2) Provide credit monitoring services to individuals whose data was under the control of the OTA Entity or resided in the OTA Entity IT system at the time of the sensitive information incident for a period beginning the date of the incident and extending not less than 18 months from the date the individual is notified. Credit monitoring services shall be provided from a company with which the OTA Entity has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

(iii) Alerts provided to the individual for changes and fraud; and

(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

(3) Establish a dedicated call center to the extent required by applicable law. Call center services shall include:

(i) A dedicated telephone number to contact customer service within a fixed period;

(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;

(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and

(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

Certification of Sanitization of Government and Government Activity-related Files and Information.

As part of contract closeout, the OTA Entity shall submit the certification to the Telos ID PM and Telos ID Contracts Administrator following the template provided in NIST Special Publication 800-88 Guidelines for Media Sanitization.

(End of clause)

OTA Entity shall take appropriate measures to protect proprietary, privileged, or otherwise confidential information that may come into their possession as a result of this Agreement.

ARTICLE XX – PRIVACY ACT

(a) The OTA Entity 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 OTA Entity 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 OTA Entity 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.

PRIVACY ACT NOTIFICATION

The OTA Entity 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.

ARTICLE XXI – DATA STORAGE AND USAGE

All applicant data collected and stored by the OTA Entity for the purpose of applying for TSA PreCheck® must be held in a separate database that can follow TSA prescribed data retention requirements. Data received and collected for the benefit of the Government shall be maintained in accordance with National Archives and Records Administration (NARA) guidelines.

The OTA Entity shall not use data collected from TSA applicants for any purpose other than submission to TSA unless the OTA Entity obtains express permission from TSA through the Telos PM as well as from each individual applicant after completion of the enrollment process for TSA PreCheck® .

The OTA Entity must clearly distinguish the completion of the enrollment process for TSA PreCheck® before requesting permission from applicants to continue communication regarding any other marketing opportunities not affiliated with TSA PreCheck® . Any such marketing communications would require the applicants to affirmatively opt-in to such additional marketing. OTA Entity is prohibited from using, in any capacity, information pertaining to an applicant's eligibility determination for TSA PreCheck® . 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.

TSA recognizes that the OTA Entity may perform other functions for applicants that rely on utilizing the same applicant data elements. All concepts that require using applicant data for purposes outside of submission to TSA require written approval from TSA through the Telos PM communication channel. Additionally, the OTA Entity must obtain and store written authorization from each applicant to use the applicant's biographic or biometric data for any purposes beyond those directly related to TSA PreCheck® and must segregate TSA data from other data that the Entity may maintain on the same applicant even where the same data element (e.g., name) appears. The OTA Entity shall operate a "system of records" within the Privacy Act of 1974, 5 U.S.C. 552a, that limits the authorized disclosure and use of TSA data.

ARTICLE XXII – INTERRELATIONSHIPS OF OTA ENTITY

OTA Entity will represent itself as an independent entity, and not as an affiliate of the TSA or DHS. Any use of the TSA PreCheck® trademark on OTA Entity Materials shall include the following or similar credit, as appropriate:

"OTA Entity is not a government entity or affiliated with the Federal government. OTA Entity provides pre-enrollment services for the Transportation Security Administration's TSA PreCheck® Risk Based Screening Program. The TSA PreCheck® 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 OTA Entity acknowledges that use of the Mark does not constitute an endorsement by DHS. TSA or the U.S. Government of OTA Entity and that OTA Entity will not state or imply that TSA, DHS or any entity of the U.S. Government endorses the OTA Entity or the goods and services associated with OTA Entity.

ARTICLE XXIX – SECTION 504 COMPLIANCE (APR 2017)

OTA Entity shall comply fully with Section 504 of the Rehabilitation Act of 1973, as amended, which prohibits discrimination against qualified individuals with disabilities. No otherwise qualified individual with a disability shall, solely by reason of his or her disability, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity for which the Entity/Provider is awarded a contract and/or receives Federal financial assistance from the Transportation Security Administration. This includes, but is not limited to, providing reasonable accommodations and effective communication to persons with disabilities and ensuring physical accessibility to all participants. The Entity/Provider shall ensure this requirement flows to all affected subcontracts.

ARTICLE XXV – THE LICENSING OF THE TSA PRECHECK® TRADEMARK

1. The TSA PreCheck® 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. DHS hereby confers to the OTA Entity a nonexclusive, nontransferable, royalty free use of the TSA PreCheck® 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 OTA Entity's marketing to prospective TSA PreCheck® Program members. The OTA Entity shall be allowed to use the DHS "TSA PreCheck® " trademark for advertising and promotional purposes in support of the TSA PreCheck® Application Program and prospective members. Such use of this trademark shall include, but is not limited to: customer communications, advertising and marketing efforts and materials, internal materials, legal disclosures, customer statement marketing (e.g. statement message, statement ad, statement insert, etc.), direct mail, letters, emails, flyers, postcards, online webpages, online secure session pages, internal communication, training tools/reference materials, account agreements, terms and conditions disclosures, Guide to Benefits, or other uses as specifically authorized in writing by TSA. Any partnership marketing efforts or promotional tie-ins involving the TSA PreCheck® Application Program must be reviewed and approved by TSA prior to implementation. Marketing messaging must maintain the integrity of the product (expedited airport security screening) and product extensions or enhancements that infer an association with security screening services or expedited screening for a purpose other than aviation security will not be allowed (e.g., expedited screening or entry services where TSA PreCheck® enrollment or status is used in place of or to expedite a non-aviation security screening. For example, TSA PreCheck® "fast lanes" or "TSA PreCheck® VIP lanes" at large events, stadiums, etc.). In addition, the OTA Entity shall provide to TSA all marketing and advertising plans for review and approval prior to launch to ensure acceptable positioning/placement of the TSA PreCheck® brand within the media marketplace and for maximum synergy with TSA-led efforts.

To maintain the legal protections associated with the trademark, TSA on behalf of DHS must control the use of the trademark. OTA Entity agrees that no modifications to DHS Materials, if provided, will be published without TSA review and prior written approval from TSA (email communication is sufficient) other than the inclusion of [Entity Name]'s logos and other necessary data. OTA Entity 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 PreCheck® trademark. Accordingly, such marketing materials shall 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 PreCheck® trademark, i.e., dilution by "blurring" and/or dilution by "tarnishment", for Materials created by OTA Entity regarding participation in the TSA PreCheck® Program, OTA Entity 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.

2. OTA Entity will represent itself as an independent entity, and not as an affiliate of the TSA or DHS. Any use of the TSA PreCheck® trademark on OTA Entity Materials shall include the following or similar credit, as appropriate:

"OTA Entity is not a government entity or affiliated with the Federal government. OTA Entity provides pre-enrollment services for the Transportation Security Administration's TSA PreCheck® Risk Based Screening Program. The TSA PreCheck® 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 OTA Entity is authorized by TSA to sub-license the TSA PreCheck® trademark to other organizations or agencies. OTA Entity will provide the TSA POC below with bi-annual reports listing all organizations with whom the OTA Entity has partnered to market the TSA PreCheck® Program.

The OTA Entity acknowledges that use of the Mark does not constitute an endorsement by DHS. TSA or the U.S. Government of OTA Entity and that OTA Entity will not state or imply that TSA, DHS or any entity of the U.S. Government endorses the OTA Entity or the goods and services associated with OTA Entity.

OTA Entity shall agree to and abide by the TSA PreCheck® License agreement incorporated hereto as Exhibit E.

ARTICLE XXX – INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING

(a) Applicability. This clause applies to the OTA Entity, its subcontractors, and OTA Entity employees (hereafter referred to collectively as "OTA Entity"). The OTA Entity shall insert the substance of this article in all subcontracts.

(b) Security Training Requirements.

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that OTA Entity employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new OTA Entity employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The OTA Entity shall maintain copies of training certificates for all Entity and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each OTA Entity and subcontractor employee shall be provided to the Telos ID PM not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to Telos ID PM via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Entity and subcontractor employees.

(2) The DHS Rules of Behavior apply to every DHS employee, OTA Entity and subcontractor that will have access to DHS systems and sensitive information. The DHS Rules of Behavior shall be signed before accessing DHS systems and sensitive information. The DHS Rules of Behavior is a document that informs users of their responsibilities when accessing DHS systems and holds users accountable for actions taken while accessing DHS systems and using DHS Information Technology resources capable of inputting, storing, processing, outputting, and/or transmitting sensitive information. The DHS Rules of Behavior is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Unless otherwise specified, the DHS Rules of Behavior shall be signed within thirty (30) days of contract award. Any new OTA Entity employees assigned to the contract shall also sign the DHS Rules of Behavior before accessing DHS systems and sensitive information. The OTA Entity shall maintain signed copies of the DHS Rules of Behavior for all Entity and subcontractor employees as a record of compliance. Unless otherwise specified, the OTA Entity shall e-mail copies of the signed DHS Rules of Behavior to the COR not later than thirty (30) days after contract award for each employee. The DHS Rules of Behavior will be reviewed annually and the Telos ID PM will provide notification when a review is required.

(c) Privacy Training Requirements. All OTA Entity and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take Privacy at DHS: Protecting Personal Information before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new OTA Entity employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The OTA Entity shall maintain copies of training certificates for all OTA Entity and subcontractor employees as a record of compliance. Initial training certificates for each OTA Entity and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the Telos ID PM via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all OTA Entity and subcontractor employees.

ARTICLE XXXI – EMPLOYMENT ELIGIBILITY VERIFICATION

The OTA Entity is required to enroll in the E-Verify program within 30 days of OTA award, if not enrolled at the time of award. For each employee assigned to the OTA, the OTA Entity shall initiate verification within 90 calendar days after date of OTA award or within 30 calendar days of the employee's assignment to the OTA, whichever date is later.

ARTICLE XXXII – REQUIRED FEDERAL PROCUREMENT PROVISIONS

The Entity and its subcontractors shall comply with the following:

1.0 Title VI of the Civil Rights Act of 1964 relating to nondiscrimination in federally assisted program.

2.0 Contracts awarded by the Provider of this Project must comply with all provisions established by laws and statutes.