SECTION II – STATEMENT OF WORK

Product, Service or Outcome Needed:

The Transportation Security Administration (TSA) Chief Diversity, Equity, Inclusion and Accessibility Officer (CDEIAO) requires Gartner subscriptions for DEIA market research, including, but not limited to, data insights and metrics, trends, challenges, and best practices. described below under "Product, Service or Outcome Needed." The requirement is for 24/7 access to the online material for a period of **Base Year (twelve months)**, beginning on **August 1, 2024**.

Purpose

The Transportation Security Administration (TSA) Chief Diversity, Equity, Inclusion and Accessibility Officer (CDEIAO) requires Gartner subscriptions for DEIA market research, including, but not limited to, data insights and metrics, trends, challenges, and best practices.

The purpose of this Statement of Work (SOW) is to procure a total of 5 license types in accordance to the schedule below. Five (5) individual licenses providing users with access to Commercially Available on-line service Gartner Subscriptions under FEDLINK.

Five (5) user subscriptions shall be dispensed in the following manner:

TSA Office	Quantity
Gartner for Chief Human Resources Officers – Team Leader	1
Gartner for Chief Human Resources Officers – Team Advisor Mem	4

24-hour online availability, 7-days a week

Background

The Transportation Security Administration (TSA) is preparing to release its People and Culture Roadmap. The Roadmap articulates TSA's goals and objectives to promote diversity, equity, inclusion, and accessibility (DEIA) throughout the agency. This Roadmap was developed by gathering input and advice from subject matter experts and employees to guide TSA's continued DEIA efforts towards a more inclusive and diverse organization.

The Roadmap outlines specific goals and objectives. Acting on the goals it sets forth will ensure TSA accomplishes the important task of protecting the traveling public while remaining a fair and equitable organization.

DEIA focuses on our people and our culture, and involves seeking systemic change within

an organization to make it more inclusive and welcoming. DEIA goes beyond "counting beans," i.e., demographic data, and seeks to understand the "why" behind this data. DEIA is a continuous process of positive change that impacts everyone. DEIA is a constant journey, whereby a culture focuses on inclusion, understanding, and belonging.

DEIA is the responsibility of the entire workforce, and this Roadmap will ensure TSA's goals are met. It is critical for the agency's success to recognize and empower programs and initiatives that are inclusive of the workforce's diverse backgrounds and experiences, as this makes TSA a resilient, innovative, and effective leader in transportation security.

PURPOSE

The Transportation Security Administration (TSA) Chief Culture Officer requires contracted services from an industry partner with a proven and traceable track record in research and advisory services to support executive Culture Office leadership in order to advance the agency's priorities to create an inclusive workforce. The Chief Culture Officer has a specific need for DEIA market research, including, but not limited to, data insights and metrics, trends, challenges, and best practices.

SCOPE

The contractor shall provide to the TSA Chief Culture Officer DEIA-focused research and tailored support on DEIA-focused functional and management issues to support executive Culture Office leadership in order to advance the agency's priorities to create an inclusive workforce. The contractor shall provide an ongoing advisory relationship that includes subject matter expert advisors and access to emerging research covering impactful evidence from the DEIA sector and

experts in government and private-sector organizations. Specifically, the contractor shall provide DEIA research, templates, functional diagnostics, case studies, peer benchmarks, peer networking, and other educational avenues.

OBJECTIVES

The contractor shall provide advisory services to the Chief Culture Officer that help transform strategies to meet the changing expectations of the global workforce and the realities of work present today and in future TSA operations. The contractor shall provide usable, relevant research, best practices, and expert analysis that address a variety of DEIA topics and trends, specifically:

DEIA Change Management. The contractor shall support TSA's DEIA implementation to achieve talent and business outcomes by providing both DEIA subject-matter expertise and executive- level change management support.

DEIA Strategy. The contractor shall assist in building a sustainable, employee-centric DEIA

strategy that aligns DEIA goals and objectives to TSA mission objectives and clearly identifies both the current state of DEIA and measures for progress.

DEIA Metrics and Accountability. The contractor shall determine appropriate metrics to track, ensuring leader accountability and assessing progress against goals.

DEIA Training and Communications. The contractor shall provide advisory services that help leaders create inclusive workplaces.

Employee Resource Groups and Executive Councils. The contractor shall provide advisory services on the creation of opportunities for employees to engage with and own DEIA strategy and how these opportunities are implemented as well as provide an analysis of outcomes.

SPECIFIC REQUIREMENTS

5.1 TASK ONE: Executive-Level Support for the Chief Culture Officer The contractor shall:

- Provide an Executive Partner. The contractor shall provide a senior-level practitioner who understands the Chief Culture Officer's role and responsibilities based on first-hand experience. The Executive Partner shall hold regular strategy meetings with the Chief Culture Officer and Culture Office staff, as appropriate.
- Conduct Virtual Strategy Meetings. The Executive Partner shall lead virtual meetings to review and apply relevant DEIA research content; recommend appropriate research experts; and develop, discuss progression of, and support modification of strategic plans.
- Facilitate Networking. The contractor shall arrange meetings on specific topics with SME peers to discuss best practices or areas of expertise.
- Provide Access to Experts. The contractor shall participate in inquiries with the Chief Culture Officer and Culture Office team members to provide personalized support on critical projects.

5.2 TASK TWO: Team Advisory

Services The contractor shall

provide the following:

- Personalized Service. The contractor shall provide a dedicated service delivery team to proactively provide relevant content and data.

- Individual Analyst Inquiries. The contractor shall provide access to experts for personalized support on critical projects.

- Unique Research in DEIA Development. The contractor shall provide access to insightful research to help the Culture Office evaluate new issues and challenges in the

following areas: diversity, equity, and inclusion; employee experience; DEIA functional strategy; leader and managerial effectiveness; change management; organizational culture; and employee well- being.

- Peer and Practitioner Research. The contractor shall provide access to peer benchmark data on efficient resource allocation, insights into leading practices, and tested approaches to solving business challenges.

- Templates. The contractor shall provide access to step-by-step guidance to execute key projects and initiatives in easy-to-use formats.

- Functional Diagnostics. The contractor shall provide custom, actionable views of key performance metrics to diagnose the current state of the key projects and initiatives.

6. PERIOD OF PERFORMANCE

The period of performance for all services shall be one year.

7. GOVERNMENT FURNISHED INFORMATION

TSA will provide the contractor with necessary information required to perform the outlined services. The contractor shall, at all times, protect and preserve all materials, information, data, supplies and equipment of every description, including that which be Government-furnished or Government-owned, from loss, damage, or harm. All resources and information provided and
generated under this contract remain the property of the Government. TSA will provide the following:

- TSA policies, management directives, and guidance regarding position management and classification.

8. GOVERNMENT FURNISHED RESOURCES

8.1 The Government will furnish information on TSA policies, existing procedures, laws, policies and operational processes when practical. When not feasible, the contractor shall conduct the necessary research to obtain the needed information.

8.2 The contractor shall use, as necessary, the TSA HC and Federal laws, regulations, policies, directives, guidance materials and case law in support of performing tasks outlined in herein.

Period of Performance:

User subscriptions will provide online access for a period of a Base Year (12 months), beginning on August 1, 2024.

Point of Contact:

[redacted]

[redacted]

SECTION III – CONTRACT ADMINISTRATION / TSA TERMS AND CONDITIONS

Type of Contract: Firm Fixed Price (FFP) FedLink Delivery Order

Contract Terms and Conditions: The Delivery Order will be subject to the terms and conditions of the awardee's FedLink contract which is administered by the United States Library of Congress.

THE FOLLOWING CLAUSES AND SUPPLEMENTAL TERMS AND CONDITIONS ARE APPLICABLE.

SUBMISSION OF INVOICES (MAY 2022)

Background: The Transportation Security Administration (TSA) partners with the United States Coast Guard Finance Center for financial services in support of TSA operations, including the payment of contractor invoices. Therefore, all contractor invoices must be submitted to, and will be paid by, the
U.S. Coast Guard Finance Center (FinCen).

Invoice Submission Method: Invoices may be submitted via U.S. Mail, or email. Contractors shall utilize ONLY ONE method per invoice submission. The submission information for each of the methods is as follows in order of preference:

It is the responsibility of the contractor to verify that invoices are received, regardless of the method of submission used. Contractors may inquire regarding the receipt of invoices by contacting the U.S. Coast Guard Finance Center via the methods listed under Payment Status below.

1. Address to mail invoices:
   United States Coast Guard Finance Center TSA Commercial Invoices
   P.O. Box 4111
   Chesapeake, VA 23327-4111

2. Email Address: [redacted]

Invoice Process: Upon receipt of contractor invoices, FinCen will electronically route invoices to be appropriate TSA Contracting Officer's Representative and/or Contracting Officer for review and approval. Upon approval, the TSA will electronically route the invoices back to FinCen. Upon receipt of certified invoices from an Authorized Certifying Official, FinCen will initiate payment of the invoices.

Discounts on invoices. If desired, the Contractor should offer discounts directly upon the invoice submitted, clearly specifying the terms of the discount. Contractors can structure discounted amounts for payment for any time period less than the usual thirty-day payment period specified under Prompt Payment requirements; however, the Contractor should not structure terms for payment of net amounts invoiced any sooner than the standard period required under FAR Subpart
32.9 regarding prompt payments for the specified deliverables under contract.

Discounts offered after invoice submission. If the Contractor should wish to offer a discount on a specific invoice after its submission for payment, the Contractor should submit a letter to the Finance Center identifying the specific invoice for which a discount is offered and specify the exact terms of the discount offered and what time period the Government should make payment by in order to receive the discount. The Contractor should clearly indicate the contract number, invoice number and date, and the specific terms of the discount offered. Contractors should not structure terms for net amount payments any sooner than the standard period required under FAR Subpart
32.9 regarding prompt payments for the specified deliverables under contract.

Payment Status: Contractors may inquire on the payment status of an invoice by any of the following means:

1. Via the internet: https://www.fincen.uscg.mil

Contacting the FinCen Customer Service Section via telephone at 1-800-564-5504 or (757) 523-6940 (Voice Option #1). The hours of operation for the Customer Service line are 8:00 AM to 5:00 PM
Eastern Time, Monday through Friday. However, the Customer Service line has a voice-mail feature that is available 24 hours per day, 7 days per week.

2. Via the Payment Inquiry Form: https://www.fincen.uscg.mil/secure/payment.htm

Invoice Elements: Invoices will automatically be rejected if the information required in subparagraph (a)(2) of the Prompt Payment Clause, contained in this Section of the Contract, including EFT banking information, Taxpayer Identification Number (TIN), and SAM-issued Unique Entity Identifier (UEI) are not included in the invoice. All invoices must clearly correlate invoiced amounts to the corresponding contract line item number and funding citation. The Contractor shall work with the Government to mutually refine the format, content and method of delivery for all invoice submissions during the performance of the Contract.

Supplemental Invoice Documentation: Contractors shall submit all supplemental invoice documentation (e.g. copies of subcontractor invoices, travel vouchers, etc.) necessary to approve an invoice along with the original invoice. The Contractor invoice must contain the information stated in the Prompt Payment Clause in order to be received and processed by FinCen. Supplemental invoice documentation required for review and approval of invoices may, at the written direction of the Contracting Officer, be submitted directly to either the Contracting Officer, or the Contracting Officer's Representative. Note for "time-and-material" type contracts: The Contractor must submit the following statement with each invoice for labor hours invoiced under a "time-and-materials" type contract, order, or contract line item: "The Contractor hereby certifies in accordance with paragraph(c) of FAR 52.232-7, that each labor hour has been performed by an employee (prime or subcontractor) who meets the contract's specified requirements for the labor category invoiced."

Additional Invoice Preparation Instructions for Software Development and/or Hardware. The Contractor shall clearly include a separate breakdown (by CLIN) for any software development activities (labor costs, subcontractor costs, etc.) in accordance with Federal Accounting Standards Advisory Board Statement of Federal Financial Accounting Standards Number 10 (Preliminary design costs, Development costs and post implementation costs)

and cite payment terms. The contractor shall provide make and model descriptions as well as serial numbers for purchases of hardware and software (where applicable.)

Frequency of Invoice Submission. This area is for the CO to document how often the contractor is allowed to submit invoices. An example is" Invoices shall be submitted on a monthly basis in accordance with the schedule." *Please note that it is desired that an invoice be tied to a deliverable.*

Timely Submission of Invoices: In order to ensure reimbursement under this contract, invoices shall be timely submitted for payment. Contractors must submit an invoice to the payment office as indicated for all allowable and allocable internal expenditures made during the specified invoice period pursuant to the Contract. Also be advised that under 31 U.S.C. §§ 1552 and 1553, funds that were obligated to the contract, but that have expired, remain available for adjustments for five (5) fiscal years following expiration of the period for which the relevant appropriation was made. After
the respective timeframe, the expired account closes and the funds are not available for any purpose.

(End of term)

CONTRACTOR PERSONNEL ACCESS TO TSA FACILITIES, INFORMATION AND/OR SYSTEMS (SEP 2020)

A. All Contractor personnel requiring access to TSA facilities, information systems, and/or information will be subject to the security procedures set forth in this contract.

B. All contractor employees seeking to provide services to TSA under a TSA contract are subject to a fitness determination to assess whether their initial employment or continued employment on a TSA contract protects or promotes the efficiency of the agency. TSA, by and through the Law Enforcement/Federal Air Marshall Service's, Personnel Security Section (PerSec), will allow a contractor employee to commence work on a TSA contract only if a review of the contractor employee's preliminary background check is favorable. Contractor employees with unfavorable preliminary background checks will not be allowed to work on a TSA contract.

C. A fitness determination involves the following three phases:

1. Phase 1: Enter On Duty Fitness Determination: a review of a contractor employee's consumer credit report, criminal history records, and submitted security forms to determine, to the extent possible, if the contractor employee has bad debt and/or criminal offenses and/or falsification issues that would prohibit employment as a TSA contractor. This determination may include verification of citizenship for contractor employees born outside of the United States. A favorable Enter On Duty Suitability Determination is not a final fitness determination; rather, it is a preliminary review of external data sources that allows the contractor employee to commence work prior to the required background investigation being completed.

When a contractor employee is deemed eligible to commence work on a TSA contract, TSA PerSec will notify the appropriate Contracting Officer's Representative (COR) of the favorable determination.
Similar notifications will be sent when a contractor employee has not passed the preliminary background check and has been deemed unsuitable.

2. Phase 2: Background Investigation: Once the contractor employee commences work on a TSA contract, TSA PerSec 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. Contractor employees who have a federal investigation sufficient in scope will immediately be processed for fmal fitness adjudication. Those contractor employees who do not have a previous federal background investigation sufficient in scope will be scheduled for the appropriate level background investigation through the National Background Investigations Bureau.

3. Phase 3: Final Fitness Adjudication: TSA PerSec will complete the final fitness determination after receipt, review, and adjudication of the completed OPM background investigation. The final fitness determination is an assessment made by TSA PerSec 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 employee has been deemed unfit for continued contract employment and that he/she shall be removed from the TSA contract.

D. The period of performance may begin 60 days after contract award to allow for the Enter On Duty Fitness Determination. A contract modification shall be executed to revise the period of performance once the determination process is completed. For Fixed price awards, in the event of staggered completed determinations the parties may negotiate fixed monthly rates so that performance can begin with partial staff.

E. Whenever personal identity verification (PIV) cards are required for issuance or re-issuance to contractor personnel for authorized access to Government facilities, under the guidance of the Contracting Officer's Representative (COR), the Contractor is responsible for making all arrangements for affected Contractor personnel to report in-person at the nearest Government issuing facility to initiate and complete procedures for PIV card issuance. The Government will not be able to provide PIV card issuance at any other locations than those officially designated as available. PIV card issuing facilities that are available for the completion of this requirement for TSA contractors are as listed by the TSA Personnel Security Section, and the COR will advise the Contractor about Government PIV card issuing facility locations that are nearby the contractor's location(s) of performance that will be potentially available for card issuance when required.

If the contractor will require access to Government Information Systems, include following paragraphs:

F. 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 representative for retention for the duration of the contract.

G. 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 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.

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.

H. 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 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 non- disclosure agreement unless otherwise authorized in writing by the Contracting Officer.

I. 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.

J. All Contractor personnel with TSA IT accounts requiring unescorted access to TSA facilities, information systems, or information will be required to complete Workplace Violence Prevention training available through the TSA Online Learning Center. The course, entitled "Preventing Workplace Violence at TSA" shall be completed within 60 days of onboarding.

(End of term)

REQUIREMENTS FOR HANDLING SENSITIVE SECURITY INFORMATION (SSI) (JUN 2021)

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. TSA, however, primarily uses the criterion of "detrimental to the security of transportation" when determining whether information is SSI.

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/). Persons authorized to access specific SSI (i.e., covered persons) include those contracted to DHS or TSA with a need-to-know basis for specific information in the course of fulfilling their TSA contractual obligations. TSA may deliver SSI materials to the Contractor. Also, materials created by the Contractor may require SSI designation and protection, and the Contractor has the responsibility to identify such materials to TSA as possible SSI. For guidance while working on TSA and DHS matters, see the TSA SSI Application Guide, 2011_04_01 for identifying the type of information covered by the regulation.

For purposes of this clause, the term "Contractor" shall include an individual or other legal entity who performs work for or on behalf of TSA or DHS under a contract, interagency agreement, or other transaction agreement. Such contracts include, but are not limited to, contracts between any non- Federal entity and/or TSA or DHS and subcontracts, joint venture agreements, and teaming agreements between any non-Federal entity and another non-Federal entity toperform work related to the primary contract with the TSA or DHS.

While SSI is not classified national security information subject to the handling requirements governing classified information, it is subject to certain legal disclosure limitations. To ensure regulatory compliance, the Contractor shall be subject to the following requirements and include this entire clause as flow-down in subcontracts, etc.:

(a) **Handling and Safeguarding.** The TSA Contractor 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. These safeguarding procedures shall include SSI recognition, identification and marking of materials that possibly contain SSI, including Contractor- created materials, as well as following restrictions on disclosure, storage, handling, sharing, dissemination and destruction of SSI. The Contractor, without exception, shall place this requirement in all subcontracts, joint venture agreements, and teaming agreements related to the performance of this contract.

(b) **Non-Disclosure Agreements (NDAs).** The Contracting Officer will provide the non-disclosure form (DHS Form 11000-6), as necessary, to the Contractor when circumstances warrant. NDAs are required to be signed by all Contractor personnel when access to SSI is necessary for performance of the contract. 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.

(c) **Request for Access to SSI materials.** Pursuant to 49 C.F.R. Part 1520.9(a)(3), the Contractor must contact [redacted] for guidance on handling requests to access to SSI (before using SSI materials) for any other purpose besides activities falling within the scope of the contract by other persons, including requests from experts, consultants, and legal counsel ("requesters") hired by the Contractor. The Contractor shall include the Contracting Officer (CO) and Contracting Officer Representative (COR) as a carbon copy "cc" recipient of its contact to [redacted] The TSA SSI Office must first make a determination as to whether the requesters are a "covered person" with a "need to know" under 49 C.F.R. Parts 1520.7 and 1520.11. Special request processing and handling requirements apply to contractor employees who may be foreign nationals. The Contractor must clearly identify any employees who are not US citizens who are otherwise requested to have access

to SSI; the requirements of TSA Management Directive 2810.3"Management of Foreign Access to Sensitive Information" apply.

(d) **Training and Certification.** All Contractor personnel who are covered persons with a need-to-know basis must complete the TSA-mandated SSI Awareness Training course prior to accessing SSI, and on an annual basis for the duration of the contract or for the duration of the requester's need for access to SSI, whichever is later. Contractor personnel must also review and adhere to the SSI Quick Reference Guide for DHS Employees and Contractors. The Contractor shall certify to the Contracting Officer annually that all covered persons have completed the mandated SSI training, that all SSI policies and procedures have been followed, and that those individuals with access understand their responsibilities to protect the information.

(e) **Breach.** In accordance with 49 C.F.R. Part 1520.9(c), the Contractor 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 Contractor shall immediately, and in no event later than one hour of discovery, report the breach to the Contracting Officer and the COR. The Contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government officials.

In the event that an SSI breach occurs as a result of the violation of a term of this contract by the Contractor or its employees, or the Contractor's covered persons, the Contractor shall, as directed by the Contracting Officer and at no cost to the Government, without delay correct or mitigate the violation.
For unauthorized disclosure of SSI, the Contractor and Contractor's employees and Contractor's covered persons may also be subject to civil penalties and other consequences as set forth in 49 CFR Part 1520.17.

(*End of term*)

NON-FEDERAL ACCESS TO TSA NATIONAL CAPITAL REGION FACILITIES (SEP 2020)

Background. Department of Homeland Security (DHS) Visitor Access Policy mandates that visitors, to include all parties such as proposed subcontractors, accessing DHS National Capital Region (NCR) Component Headquarters and related Headquarters NCR facilities be subject to a criminal history check. To that end, in July 2016, TSA began requiring the submission of Personally Identifiable Information (PII) for all non-federal visitors and foreign national visitors entering TSA facilities in the National Capital Region, including TSA Headquarters, the Freedom Center, Annapolis Junction, Walker Lane, and the Transportation Security Integration Facility (TSIF), in order to process the required screening checks. Of note, for contracts requiring access to TSA facilities, information systems, or sensitive but unclassified information as part of contract performance, contractor employees are subject to a suitability determination.

(a) Purpose: The submitted information will be used to conduct screening checks to permit and maintain records of access to DHS NCR facilities pursuant to the authority of 40 U.S.C. § 1315; 41
C.F.R. Part 102-81; Executive Order. 9397.

(b) Applicability: A Non-Federal Visitor or Foreign National Visitor is an individual who has not been issued a DHS Personal Identity Verification (PIV) card or is not a current Federal government

employee. Non-TSA current Federal government employees will be recorded in the Visitor Request Form excluding any PII.

(c) Routine Uses: The information requested may be shared externally as a "routine use" to the Department of Justice, Federal Bureau of Investigation and other government agencies as part of the screening process. A complete list of the routine uses can be found in the system of records notice, "Department of Homeland Security/ALL-024 Facility and Perimeter Access Control and Visitor Management System of Records."

(d) Consequences of Failure to Provide Information: Providing this information, including Social Security Number (SSN), is voluntary. However, failure to provide the information requested may result in being denied access to a DHS facility; failure to provide the SSN may prevent completion of screening.

(e) Information Requirements. In accordance with the above:

1. Non-Federal Visitors. Non-Federal visitors to TSA facilities will need to provide Date of Birth and Social Security Number information. The required information shall be provided in a password protected Microsoft Excel spreadsheet emailed to the Contracting Officer at least one (1) full business day prior to the visit date. (For further information, the Contracting Officer is a federal government employee who is specifically authorized and appointed in writing under specified agency procedures and granted the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.) The Contracting Officer may delegate the receipt of this information to the respective Contracting Officer Representative (COR). In order to ensure protection of this information, the password for the password protected spreadsheet shall be sent to the Contracting Officer (or delegated COR) in a separate email, at the same time. If multiple non- federal visitors from one company require access to TSA Headquarters facilities, that company should submit a single complete spreadsheet. A DHS/TSA employee shall be responsible for both inputting the information into the Visitor Request Form and actual escorting the visitor(s) at all times. The submitted emails shall then be deleted by TSA.

2. Foreign National Visitors. Foreign Nationals visiting TSA facilities in the U.S. and its territories will need to submit additional information to screening purposes, specifically:

- Date of Birth
- Gender
- Country of Citizenship
- Country of Birth
- Passport Number and Expiration Date
- Position/Title

The required information shall be provided in a password protected Microsoft Excel spreadsheet emailed to the Contracting Officer at least seven (7) full business days prior to the visit date. The Contracting Officer may delegate the receipt of this information to the respective Contracting Officer Representative (COR). In order to ensure protection of this information, the password for the password protected spreadsheet shall be sent to the Contracting Officer (or delegated COR) in a

separate email, at the same time. If multiple Foreign National visitors from one company require access to TSA Headquarters facilities, that company should submit a single complete spreadsheet. A DHS/TSA employee shall be responsible for both inputting the information into the Visitor Request Form and actual escorting the visitor(s) at all times. The submitted emails shall then be deleted by TSA.

(End of term)

PERFORMANCE BY FOREIGN NATIONAL CONTRACTOR EMPLOYEES (SEP 2020)

Special request processing and handling requirements apply to contractor employees who may be foreign nationals. The Contractor must clearly identify any employees who are not US citizens who are otherwise requested to have access to SSI; the requirements of TSA Management Directive 2810.3"Management of Foreign Access to Sensitive Information" apply. Notwithstanding the requirements in HSAR 3052.204-71, Contractor Employee Access, contractors who propose to have contract work performed by contractor employees who are not United States Citizens or Lawful Permanent Residents and who will have access to sensitive but unclassified information performance of their job shall be required to submit biographical information (e.g. name, date of birth, passport information, etc.) for vetting purposes.

The required vetting must occur both prior to the start of the contract, and annually thereafter. As such, the contractor must submit the necessary biographical information no later than ninety (90) days prior the start of the contract and prior to the end of the contract's annual performance period. In the event such Contractor employees are no longer utilized for performance under the contract, the Contractor shall notify the Contracting Officer and Contracting Officer Representative (COR) by xx day and begin the replacement of personnel and vetting. The re-vetting of all said current personnel shall remain on the above annual schedule. Please note that this requirement under this contract's Key Personnel clause(s) for any non-United States Citizens or Lawful Permanent Residents that are deemed key personnel remain in effect.

This annal vetting process requirement does not and will not affect the Government's separate and unilateral discretion on whether to exercise the contract's option(s) to extend the contract nor the Contracting Officer's discretion on whether to issue a notification to exercise the contract's option period. The administrative requirement for contractor submission of vetting information (along with any vetting clearance results) will have no relationship as to whether the Contracting Officer issues a notice of intent to exercise an option and the Government's discretion to exercise the option.

The required information shall be provided in a password protected Microsoft Excel spreadsheet emailed to the Contracting Officer. The Contracting Officer may delegate the receipt of this information to the respective COR. In order to ensure protection of this information, the password for the password protected spreadsheet shall be sent to the Contracting Officer (or delegated COR) in a separate email, at the same time. If multiple Foreign National employees from one company require vetting, that company must submit a single complete spreadsheet. All password protected submissions shall be protected by the Government and destroyed upon conclusion of the annual vetting exercise.

The Contracting Officer and/or COR will notify the contractor of the conclusion of the vetting process.

(End of term)

PUBLICITY AND DISSEMINATION OF CONTRACT INFORMATION (SEP 2020)

The Contractor 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 contract without the prior written consent of the Contracting Officer. The Contractor shall submit any request for public release at least ten (10) business days in advance of the planned release. Under no circumstances shall the Contractor release any requested submittal prior to TSA approval.

Any material proposed to be published or distributed shall be submitted 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.

(End of term)

CONTRACTOR PERSONNEL ACCESS TO TSA FACILITIES, INFORMATION AND/OR SYSTEMS (SEP 2020)

A. All Contractor personnel requiring access to TSA facilities, information systems, and/or information will be subject to the security procedures set forth in this contract.

B. All contractor employees seeking to provide services to TSA under a TSA contract are subject to a fitness determination to assess whether their initial employment or continued employment on a TSA contract protects or promotes the efficiency of the agency. TSA, by and through the Law Enforcement/Federal Air Marshal Service's, Personnel Security Section (PerSec), will allow a contractor employee to commence work on a TSA contract only if a review of the contractor employee's preliminary background check is favorable. Contractor employees with unfavorable preliminary background checks will not be allowed to work on a TSA contract.

C. A fitness determination involves the following three phases:

1. Phase 1: Enter On Duty Fitness Determination: a review of a contractor employee's consumer credit report, criminal history records, and submitted security forms to determine, to the extent possible, if the contractor employee has bad debt and/or criminal offenses and/or falsification issues that would prolnbit employment as a TSA contractor. This determination may include verification of citizenship for contractor employees born outside of the United States. A favorable Enter On Duty Suitability Determination is not a fmal fitness determination; rather, it is a preliminary review of external data sources that allows the contractor employee to commence work prior to the required background investigation being completed.

When a contractor employee is deemed eligible to commence work on a TSA contract, TSA PerSec will notify the appropriate Contracting Officer's Representative (COR) of the favorable determination.
Similar notifications will be sent when a contractor employee has not passed the preliminary background check and has been deemed unsuitable.

2. Phase 2: Background Investigation: Once the contractor employee commences work on a TSA contract, TSA PerSec 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. Contractor employees who have a federal investigation sufficient in scope will immediately be processed for fmal fitness adjudication. Those contractor employees who do not have a previous federal background investigation sufficient in scope will be scheduled for the appropriate level background investigation through the National Background Investigations Bureau.

3. Phase 3: Final Fitness Adjudication: TSA PerSec will complete the fmal fitness determination after receipt, review, and adjudication of the completed background investigation. The fmal fitness determination is an assessment made by TSA PerSec 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 fmal fitness determination will

result in a notification to the COR that the contractor employee has been deemed unfit for continued contract employment and that he/she shall be removed from the TSA contract.

D. The period of performance may begin 60 days after contract award to allow for the Enter On Duty Fitness Determination. A contract modification shall be executed to revise the period of performance once the determination process is completed. For Fixed price awards, in the event of staggered completed determinations the parties may negotiate fixed monthly rates so that performance can begin with partial staff.

E. Whenever personal identity verification (PIV) cards are required for issuance or re-issuance to contractor personnel for authorized access to Government facilities, under the guidance of the Contracting Officer's Representative (COR), the Contractor is responsible for making all arrangements for affected Contractor personnel to report in-person at the nearest Government issuing facility to initiate and complete procedures for PIV card issuance. The Government will not be able to provide PIV card issuance at any other locations than those officially designated as available. PIV card issuing facilities that are available for the completion of this requirement for TSA contractors are as listed by the TSA Personnel Security Section, and the COR will advise the Contractor about Government PIV card issuing facility locations that are nearby the contractor's location(s) of performance that will be potentially available for card issuance when required.

If the contractor will require access to Government Information Systems, you should include following paragraphs:

F. 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 representative for retention for the duration of the contract.

G. 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.

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.

H. 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 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 non- disclosure agreement unless otherwise authorized in writing by the Contracting Officer.

IF the TSA service contracts requires on-site contractor performance where contractors will have TSA IT accounts with access to the TSA Online Learning Center (OLC, you may include the following paragraph.

I. All Contractor personnel with TSA IT accounts requiring unescorted access to TSA facilities, information systems, or information will be required to complete Workplace Violence Prevention training available through the TSA Online Learning Center. The course, entitled "Preventing Workplace Violence at TSA" shall be completed within 60 days of onboarding.

(End of term)

CONTINGENCY AND/OR CONTINUITY OF OPERATIONS SUPPORT OF TRANSPORTATION SECURITY ADMINISTRATION OPERATIONS (SEP 2020)

A. Background. The Transportation Security Administration (TSA) is a component of the Department of Homeland Security (DHS) and is responsible for the security of the nation's transportation system. This includes not only the security screening operations conducted for passenger air travel, but also security operations protecting air cargo and shipping, surface and other transportation modes including rail, and pipelines and other transportation infrastructure. To those ends, the TSA must be able to respond quickly to incidents, and increase and re-constitute its operational posture ("continuity of operations") in response to threats and the possibility of actual attacks upon or disruption to government operations or national infrastructure. The TSA has an internal capacity to establish and operate Critical Incident Management Groups in response to a specific, TSA-only incident, or as a part of larger DHS operation due to orders from the DHS Secretary, or due to increased threat levels under the National Terrorism Advisory System, or federal operations up to and including responsibilities assigned under the National Response Framework. To these ends, the TSA must be able to count

upon a correlated contractor

capability to surge capacity in response to incidents or quickly re-constitute capability to recover from a catastrophe. Accordingly, TSA contractors must be prepared and able to provide surge capacity and to reconstitute operational capability to perform under contract as required in response to an emergency.

B. Definitions. The meaning of specific contingency or emergency-related terms herein proceeds from those definitions within the National Response Framework and are available from the National Response Framework Resource Center glossary athttp://www.fema.gov/emergency/nrf/.

C. Force and effect of this requirement. Without regard to the extent that the Contractor's actual responses in order to meet the requirements of this term may be necessitated by occurrences or conditions as described in the "Excusable Delays" paragraph of FAR 52.212-4, "Contract Terms and Conditions-Commercial Items" clause or those described in the FAR 52.249-14, "Excusable Delays" clause (or such related conditions as described in other clauses, such as the FAR 52.249-8 "Default (Fixed-Price Supply and Service)," 52.249-9 "Default (Fixed-Price Researchand Development)," and/or FAR 52.249-10 (Fixed-Price Construction)," if included in the contract), the Contractor shall provide surge capacity, re-establish functions, and reconstitute capability and performance under this contract as quickly as possible in response to an incident and/or as ordered by the Contracting Officer.

D. Response functions and capabilities. The Contractor shall establish and maintain the following capabilities as a requirement of this contract.

1. Continuity of Operations (COOP) Plan. The Contractor shall establish a written continuity of operations plan in accordance with "Continuity Guidance Circular 1 (CCGI), Continuity Guidance for Non- Federal Agencies" of January 2009. In general, COOP plans must be designed in order to:

a) Minimize loss of life, injury, and property damage.

b) Mitigate the duration, severity, or pervasiveness of disruptions that do occur.

c) Achieve the timely and orderly resumption of essential functions and the return to normal operations.

d) Protect essential facilities, equipment, records, and assets.

e) Be executable with or without warning.

f) Meet the operational requirements of the TSA. Continuity plans need to be operational within minutes of activation, depending on the essential function or service, but certainly should be operational no later than 12 hours after activation.

g) Meet the sustainment needs of the TSA. An organization may need to plan for sustained continuity operations for up to 30 days or longer, depending on resources, support relationships, and the respective continuity strategy adopted.

h) Ensure the continuous performance of essential functions and operations during an emergency, including those such as pandemic influenza that require additional considerations beyond traditional continuity planning.

i) Provide an integrated and coordinated continuity framework that takes into consideration other relevant organizational, governmental and private sector continuity plans and procedures.

2. The Contractor's COOP Plan is intended to be executed in response to an incident, and the COOP Plan shall address each of the following requirements in depth, in addition to the essential functions described in CCG1:

a) Communications. In the case of an applicable incident or a notification per paragraph (e) "Response Requirement" below, the Contractor shall maintain or be able to re-establish active, real-time communication with its employees under the contract during the 24-hour day period on all days during the week such that the Contractor can ensure performance under the contract will continue at such alternate locations under the contract to meet specified deliverables and/or response to surge capacity. Likewise, the Contractor shall ensure that effective communication about its contract performance can continue with the Contracting Officer, taking into account the operational profile or location of TSA facilities or assets in response to an incident in order to meet specified deliverables and/or response to surge capacity orders from the Contracting Officer.

b) Facilities. In the case of an applicable incident or a notification per paragraph (e) "Response Requirement" below, the Contractor shall be able to re-constitute contractor presence at self- provided facilities or at Government-provided facility space as may be required in order to meet specified deliverables and/or response to surge capacity orders from the Contracting Officer.

c) Information Systems/Network. In the case of an applicable incident or a notification per paragraph (e) "Response Requirement" below, the Contractor shall maintain and be able to re- constitute an information systems network at its facilities or for use at alternate facilities as may be necessary in order to meet specified deliverables and/or respond to surge capacity orders from the Contracting Officer.

d) Annual or Periodic COOP Exercise. Under the monitoring of the Contracting Officer and Contracting Officer's Representative (COR), the Contractor shall conduct an annual exercise to test the capabilities of its COOP Plan, or the Contractor may be included in periodic TSA COOP exercises as a means of fulfilling this requirement. Typically, a simulated scenario for the exercise will be developed, and the contractor's management team will place the scenario into action on a simulated basis. As with all exercises, responses to the exercise must be based on the known capacities and capabilities of the contractor's personnel and assets and take the actual disposition and locations of personnel and assets into account at the initiation and during the conduct of the exercise. Thus, while the exercise's scenario is simulated, the contractor's ability to initiate and to plan the execution of a response to the scenario via the COOP Plan is actual and will be assessed by the Government. The Contractor shall implement recommendations as a consequence of the Government's assessment of its performance in response to the exercise. The Government's assessment of COOP plan practice may be likewise included at the Government's discretion as a portion of the "management" element assessed under the Contractor Performance Assessment Reporting System. Initiation of an exercise in response to the requirements of this term does not entitle the Contractor to an equitable adjustment or otherwise constitute a change to this contract.

e) Surge capacity and Continuity of Operations (COOP). The Contractor may be required to provide either surge capacity and/or a COOP response to conditions related to this term. "Surge

capacity" means that the volume and pace of the contractor's performance is required to increase to meet the TSA's increased volume of work and tempo of operations in an emergency situation. "COOP" means that the contractor may have to conduct various activities to re- establish or reconstitute operations in response to an incident, which could also include a necessity to provide for surge capacity.

E. Response Requirement. The Contractor shall provide surge capacity to implement an increased workload within (Fill in the amount): hours of notification by the Contracting Officer in the event of:

1. a specific declaration of national emergency by the Executive Office of the President and/or the occurrence of an Incident of National Significance or Major Disaster;

2. a contingency operation initiated by DHS and/or the TSA;

3. a continuity of operations re-establishment of DHS and/or its components' locations, deployments, or operational profiles;

4. an emergency or event that affects DHS or TSA operations, requires a specific response as directed by the President, Secretary of Homeland Security, or Principal Federal Official so designated, and/or
actuates part or all of the requirements within the National Response Framework;

5. an increase in the Threat Levels published via the Homeland Security Advisory System, either on a national or an industry/sector specific basis (especially with respect to the Threat Conditions of "High," and/or "Severe"); and/or

6. the establishment of a specific TSA Critical Incident Management Group related to the functional area supported by this contract.

Staffing requirements may increase dramatically during such contingency operations or events. During the beginning of a contingency, the contractor shall be prepared to augment staffmg for the duration of the contingency in order to not impact the timeliness of other tasks, which may also be critical during a contingency.

F. Ordering Surge Support. When the contractor's support to provide surge capacity in response to the requirements of this term is required under the contract, a duly appointed and warranted Contracting Officer will order such support in writing. Only such a designated Contracting Officer is authorized to direct Contractor's performance in support of the requirements of this term.

G. Annual Statement Affirming Compliance. During each year of performance while this contract is in force, the Contractor is required to submit to the Contracting Officer, on the first day of

December or the next following business day, a statement affirming the contractor's intent to comply fully with the requirements of this term and to indicate sufficient internal capacity to do so.

H. Right to an Equitable Adjustment. This term in no way diminishes or alters the right of the Contractor to an equitable adjustment for performance initiated in response to the Contracting Officer's

(End of term)

504 COMPLIANCE (SEP 2020)

The Contractor/Provider 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 Contractor/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 Contractor/Provider shall ensure this requirement flows to all affected subcontracts.

(End of term)

SECURITY REQUIREMENTS FOR HANDLING PERSONALLY IDENTIFIABLE INFORMATION AND PRIVACY INCIDENT REPONSE (SEP 2020)

Along with this verbiage, include HSAR 3052.204-70 "Security Requirements for Unclassified Information Technology Resources" (JUN 2006), HSAR 3052.204-71, "Contractor Employee Access" (SEP 2012), and FAR 52.224-3 "Privacy Training" (JAN 2017) ALT I in the same contract.

A. Definitions.

1. "Breach" (may be used interchangeably with "Privacy Incident') as used in this term 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.

2. "Personally Identifiable Information (PII)" as used in this term 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.

3. "Sensitive Personally Identifiable Information (Sensitive PII)" as used in this term 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:

a. Driver's license number, passport number, or truncated SSN (such as last digits)
b. Date of birth (month, day, and year)
c. Citizenship or immigration status
d. Financial information such as account numbers or Electronic Funds Transfer Information

e. Medical Information
f. 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 Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The contractor shall provide the Government access to, and information regarding the contractor's systems, 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.

1. 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 the most current versions of DHS Sensitive System Publication 4300A and TSA Information Assurance (IA) Handbook or any replacement publication and rules of conduct as described in TSA Management Directive (MD) 3700.4.

2. All Contractor-operated systems that input, store, process, output, and/or transmit SPII 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 Contractor 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 with at least Advanced Encryption Standard (AES)-256 or higher 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 Contractor systems from Government tools and infrastructure.

3. 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:

a. Laptops employ encryption with at least AES-256 or higher using a NIST Federal Information Processing Standard (FIPS) 140-2 or successor approved product;

b. The contractor has developed and implemented a process to ensure that security and other applications software are kept current;
c. Mobile computing devices utilize anti-viral software and a host-based firewall mechanism;
d. When no longer needed, all removable media and laptop hard drives shall be processed (i.e., sanitized, degaussed, or destroyed) in accordance with DHS and TSA security and disposition requirements.
e. The contractor shall maintain an accurate inventory of devices used in the performance of this contract;
f. Contractor employee training requirements are covered in FAR 52.224-3.
g. 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 and TSA Information Assurance Handbook, which the contracting officer will provide upon request. Certification of data removal or data disposition 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.

1. Contractor shall limit access to the data covered by this term to those employees and subcontractors who require the information in order to perform their official duties under this contract.

2. 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.

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

E. Breach Response.
The contractor agrees that in the event of any actual or suspected breach of SPII (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 Representative (COR), and the TSA Privacy Officer (TSAprivacy@tsa.dhs.gov). The contractor is responsible for positively verifying that notification is received and acknowledged by at least one of the foregoing Government parties. The report of a breach shall not, by itself, be interpreted as evidence that the contractor failed to provide adequate safeguards for SPII.

Award fee contracts:

1. For any portions of this contract that involve an award fee, the contractor may be awarded no award fee for any evaluation period in which there is a breach of privacy or security, including any loss of sensitive data or equipment containing sensitive data. Lost award fee due to a breach of privacy or security may not be allocated to future evaluation periods.

2. For any portions of this contract that involve an award fee, to ensure that the final award fee evaluation at contract completion reflects any breach of privacy or security in an interim period, the overall award fee pool shall be reduced by the amount of the fee available for the period in which the breach occurred if a zero fee determination was made because of a breach of privacy or security.

F. Personally Identifiable Information Notification Requirement.

1. The contractor shall have 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 by the Government. 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: (i) notification is appropriate; and (ii) 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: (i) a brief description of how the breach occurred; (ii) a description of the types of personal information involved in the breach; (iii) a statement as to whether the information was encrypted or protected by other means; (iv) steps an individual may take to protect themselves; (v) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (vi) point of contact information identifying who affected individuals may contact for further information.

2. In the event that a 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 less than18 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 term, 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 term will be attributed to the contractor.

(End of term)

DHS and TSA Enterprise Architecture (December 2022):

a) The Contractor shall ensure that all architectural artifacts including but not limited to solutions, business, Data, IT elements for legacy Transportation Security Equipment (TSE), Information Systems Security Agreements (ISSAs), System Design documents (SDDs), deliverables, and services are aligned and compliant with the current DHS and TSA Enterprise Architecture, and the (The Common Approach to Federal Enterprise Architecture), the Technology Business Management (TBM) Taxonomy, and Federal Information Technology Acquisition Reform Act (FITARA).

i. All solutions and services shall meet DHS and TSA Enterprise Architecture policies, standards, and procedures. Specifically:

a. DHS and TSA Enterprise Architecture policies, standards, and procedures.

b. Homeland Security Enterprise Architecture (HLS EA) and TSA EA requirements.

c. TSA and DHS IT Security, Cloud, Infrastructure (including Network), Application/Systems, Information/Data, Performance, and Business Architecture policies, directives, guidelines, standards, segment architectures and reference architectures.

d. TSA functional capabilities

e. TSA operational capabilities

f. TSA lines of business

g. TSA business processes

h. TSA funding sources

i. TBM Taxonomy for IT cost transparency

ii. All software and tools that are used to build, develop, or deploy IT solutions for TSA, shall leverage the TSA NextGen Architecture (NGA) Technology Stack known as "The Kit". In accordance with TSA CIO Priority 2.1 "Modernize, Simplify, Reduce and Enforce TSA IT and Data Toolkit", use of "the Kit" will achieve modernization and simplification, with the ultimate goal of reducing the current TSA Technology Footprint.

iii. This includes new Transportation Security Equipment (TSE) and Legacy TSE that utilizes IT software, services, or equipment including embedded IT elements such as network switches, routers, In printers, etc.

iv. All solutions shall implement and leverage TSA information and data standards as defined and approved per TSA policy.

v. All solution architectures and services (e.g., Application, System, Network, Security, Information/Data, Cloud) shall be reviewed and approved by TSA EA as part of the TSA SELC (System Engineering Life Cycle) review process and in accordance with TSA IT Governance Management Directive 1400.20 with applicable DHS and TSA IT governance policies, directives, and processes. This includes the Solution Engineering Review (SER), Preliminary Design Review (PDR) and Critical Design Review (CDR) stage gates. The required design artifacts include solution approach document, the PDR document, and the System Design Document (SDDs) as directed by EAD. Successful completion of the PDR/CDR stages results in an approved architecture which is required before proceeding to development. An approved architecture is also a necessary critical step in receiving an Authority to Operate (ATO). 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.

vi. TSA Offices acquiring Enterprise architecture type services at segment or solution levels shall engage and collaborate with the TSA Enterprise Architecture Division (EAD) to ensure strategic alignment of people, process, information, and technology and comply with enterprise level architecture governance, artifacts and standards.

a. The Contractor shall engage domain architect(s) in EAD before SELC Obtain Phase, i.e. during SELC Need or "Analyze and Select" Phase.

b. The Contractors shall collaborate with the EA domain architect(s) to deliver the required design artifacts and desired outcome under the guidance.

c. The Contractor shall provide architecture and system/application data and models in prescribed formats to be stored in TSA's Enterprise Architecture Repository.

b) In accordance with the TSA Cloud Strategy 2.0, April 2019, TSA's approach to cloud computing and governance of migration to the cloud, the contractor shall ensure that the cloud solutions utilize the SaaS (Software as a Service) model as its primary approach to cloud implementation, and also, when necessary will use Platform as a Service (PaaS) or Infrastructure as a Service (IaaS). The contractor shall adhere to the principles of cloud strategy to systematically retire or replace legacy applications by use of an integrated approach to cloud planning, architecture, hybrid deployment, and operation.

c) 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-21-07, November 2020) 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.

Information and Data Governance and Management

d) The Contractor shall develop, use, and dispose of TSA information and data assets following the TSA governance processes established by the Enterprise Information/Data Governance Board (EIDGB), in compliance with the DHS Enterprise Data Governance and Management MD (Management Directive) 103-01.

i. TSA information and data assets include but are not limited to the TSA Data Catalog, TSA information and data standards, TSA Data Management Plan, TSA data sets (including open data sets for public consumption), TSA information and data stored in TSA repositories, TSA information and data in systems and applications (internal and external), and TSA information exchanges.

ii. All TSA information and data, and all solutions that capture, store, use and provide TSA information and data shall comply with the Geospatial Data Act (GDA) of 2018 (P.L. 115-254) that requires agencies to foster efficient management of geospatial data/information, technologies, and infrastructure through enhanced coordination among Federal, state, local, and tribal governments, along with private sector and academia.

iii. Description information for all data assets shall be submitted to the TSA Enterprise Architecture Team, who will be responsible for coordination with DHS, and for review, approval and insertion into the TSA Data Reference Model and Enterprise Architecture Repository.

iv. 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 a format understandable to TSA. Examples of data structures can be defined as, but not limited to:

a. Data models containing entities and attributes, identifying authoritative and trusted data sources, and 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
e. Information exchange specifications

v. 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 (Statement of Work), SOO (Statement of Objectives) and PWS (Performance Work Statement). This definition complies with not only the delivery of data, but also maintaining TSA-specific data within a non-TSA or DHS proprietary system.
vi. 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 version, the most current data to be used, as well as frequency of data refreshes.
vii. The contractor shall provide a Data Asset Repository Profile (DAR) and Data Management Plan (DMP) to EA using EA provided template before the preliminary/critical design review. The DAR and DMP include conceptual and logical data models, data dictionaries, data asset profile, and other artifacts pertinent to the project's data.
viii. TSA adheres to the DHS NIEM (National Information Exchange Model) First policy and standards outlined in the DHS Memorandum, "Adoption of the National Information Exchange Model within the Department of Homeland Security," dated May 3, 2019. All TSA information and data exchanges shall be NIEM compliant. All TSA solutions that

Cybersecurity Policy for TSA Government Acquisitions (May 2023)

A. General Security Requirements:

A.1. All authorized, cleared and vetted personnel (i.e., federal employees; and primary, subcontractor, and/or 3rd party vendors or contractors) supporting or doing business per agreement with TSA (either directly or indirectly) shall comply with applicable cybersecurity or information assurance (IA) policies as stated in the DHS Policy Directive 4300A, "Information Technology System Security Program, Sensitive Systems, version 13.3, Feb 23, 2023 (hereafter known as DHS 4300A); DHS National Security Systems Policy Directive 4300B Version 10.1, November 21, 2018 for classified systems (hereafter known as DHS 4300B); TSA MD 1400.3 Information Technology Security (ITS); TSA Information Assurance (IA) Handbook; supplemental Technical Standards (TSs) and Standard Operating Procedures (SOPs); TSA Cloud Computing Security Handbook (CCSH); and the DOD Cloud Computing Security Requirements Guide (CC SRG).

A.2. The Contractor shall comply with Federal, Department of Homeland Security (DHS) and Transportation Security Administration (TSA) security, sensitive information handling, and privacy guidelines in effect at the time of the award of the contract, as well as those requirements that may be added during the contract.

A.3. The Contractor shall perform periodic reviews to ensure compliance with cybersecurity, information security and privacy requirements.

A.4. The Contractor shall comply with proper DHS and TSA security controls to ensure that the Government's security requirements are met. These controls are described in DHS 4300A, TSA MD 1400.3 ITS and the TSA Information Assurance (IA) Handbook security policy documents and are based on the current National Institute of Standards and Technology (NIST) Special Publication (SP) 800-32 Rev 2 and 800-53 Rev 5 standards.

A.5. The Contractor shall include this guidance in all subcontracts at any tier where the subcontractor is performing the work defined in the Statement of Work (SOW), Performance Work Statement (PWS), Statement of Objective (SOO).

A.6. The Contractor shall ensure all of its staff members have the required level of approved security clearance commensurate with the sensitivity of the information being accessed, stored, processed, transmitted or otherwise handled by the system or required to perform the work stipulated by the contract. At a minimum, all Contractor staff shall be subjected to a Public Trust background check and be granted a Public Trust clearance before access to any system or other TSA resources as granted.

A.7. The Contractor shall sign a DHS Form 11000-6 *Non-Disclosure Agreement (NDA)* within thirty (30) calendar days of the contract start date.

A.8. The Contractor shall not release, publish, or disclose agency information to unauthorized personnel, and shall protect such information in accordance with the provisions of pertinent laws, regulations, and policies governing the confidentiality of sensitive information.

A.9. The Contractor shall ensure its staff follow all policies and procedures governing cybersecurity, physical, environmental, and information security described in the various TSA regulations pertaining thereto, and the specifications, directives, and manuals for conducting work to generate the products as required by the contract. Personnel shall be responsible for the physical security of their work area and government furnished equipment (GFE) issued to the contractor under the terms of the contract.

A.10. The Contractor shall make all system information and documentation produced (in support of the contract) available to TSA upon request.

B. Training Requirements:

B.1. All newly-arrived Contractor employees requiring system access shall receive initial "*Organizational Security Fundamentals (OSF)*" training within 60 days of assignment to the contract via the Online Learning Center (OLC). The COR shall initiate and facilitate this access. Refresher training shall be completed annually thereafter. Another required OLC cybersecurity training course is the "*Cybersecurity for TSA System Users (TSA-CYBRSCRTY-SYSTM-USRS)*" training and would be the official TSA-wide course developed in accordance with mandated policy to safeguard TSA's mission and assets. It is the annual course that all users shall take and the one leveraged against FISMA requirements. (Note: This course replaced the older animated "IT Security Awareness" training of the past).

B.2. The Contractor shall complete any TSA-related Privacy training on an annual basis.

B.3. Role-Based training is required for contract employees with Significant Security Responsibility (SSR), whose job proficiency is required for overall network security within TSA, and shall be in accordance with DHS and TSA policy. The contractor shall be notified if

they have a position with Significant Security Responsibilities.

B.4. Individuals with SSR shall have a documented individual training and education plan, which shall ensure currency with position skill requirements, with the first course to be accomplished within 90 days of employment or change of position. The individual training plan shall be refreshed annually or immediately after a change in the individual's position description requirements.

B.5. Cybersecurity and privacy training supplied by the Contractor shall meet standards established by NIST and set forth in DHS and TSA security policy.

B.6. The Contractor shall maintain an accurate and up-to-date list of all vetted contractor employees who have completed training and shall submit this list to the Contracting Officer Representative (COR) upon request, or during DHS/TSA onsite validation visits performed on a periodic basis.

B.7. The contractor shall ensure its employees review, understand, and sign the TSA Form 1403 *Computer and Wireless Mobile Device Access Agreement (CAA)* prior to accessing any IT systems.

C. Configuration Management (hardware/software/applications):

C.1. Hardware or software configuration changes shall be in accordance with the current DHS Information Security Performance Plan, 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)/Executive Director for Information Assurance and Cybersecurity Division (IAD) shall be informed of and aware of all configuration changes to the TSA IT environment including, but not limited to: systems, hardware, software, applications, infrastructure architecture, infrastructure assets, and end user assets. The TSA IAD POC shall approve any Request for Change (RFC) prior to any development activity occurring for that change and shall define the security requirements for the requested change. The COR shall provide access to the DHS Information Security Performance Plan.

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

C.3. The Contractor shall ensure all sites, facilities or operational functions 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 authorized products that have been carefully analyzed, reviewed, evaluated and validated, as appropriate, in accordance with the following:

- The NIST FIPS validation program.
- The National Security Agency (NSA)/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 Department of Defense/Department of Homeland Security, Security Technical Implementation Guides (STIGs)

a) The provider of information technology shall certify all applications are fully functional, safe, secure and operate correctly as intended on systems using the US DoD Security Technical Implementation Guides (STIGs) and in accordance with DHS and TSA guidance.

1. DoD STIGs:
    a. https://public.cyber.mil/stigs/

2. DHS Sensitive Systems Configuration Guidance:
    a. https://dhsconnect.dhs.gov/org/comp/mgmt/ocio/ciso/Pages/sscg.aspx The standard installation, operation, maintenance, management, updates and/or
    patching of software shall not alter the configuration settings from the approved USGCB configuration. The information technology shall also use the Windows Installer Service for installation to the default "program files" directory and shall be able to discretely install and uninstall.

b) Applications designed for general end users shall run in the general 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/information by ensuring all such devices are monitored by, and report to, the TSA Security Operations Center (SOC). The Contractor shall perform monthly security scans on servers that contain TSA data, and shall send monthly scan results to the TSA IAD.

D. Risk Management Framework (RMF):

D.1. The Security Authorization (SA) and Ongoing Authorization (OA) processes, in accordance with recent NIST SP 800-37 and SP 800-137, are required for all TSA IT systems, including General Support Systems (e.g., standard TSA desktop, general network infrastructure, electronic mail), 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 (RMF) and the Ongoing Authorization is part of Step 6 "Monitoring" of the RMF. All NIST guidance is publicly available; TSA and DHS security policy is disclosed upon contract award with some exceptions, which are public facing (i.e., DHS Security and Training Requirements for Contractors).

D.2. A written Authorization 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 in support of the Security Authorization (SA) process.

D.3. TSA shall assign a security category to each IT system compliant with the requirements of Federal Information Processing Standards (FIPS) Pub 199 *Standards for Security Categorization of Federal Information and Information Systems* impact levels and assign security controls to those systems consistent with FIPS Pub 200 *Minimum Security Requirements for Federal Information*

and Information Systems methodology.

D.4. Unless the AO specifically states otherwise for an individual system, the duration of any accreditation shall 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 (SA) Package contains documentation required for Security Authorizations and Ongoing Authorization. The package shall contain the following security documentation as required by the DHS Ongoing Authorization Methodology:

1) Security Assessment Report (SAR),
2) Security Plan (SP),
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

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 shall be reviewed and approved by the CISO and the IAD, and accepted by the Contracting Officer (CO) upon creation and after any subsequent changes, before they go into effect. Note: The CO shall not alter or remove any documentation or language once approved by IAD or authorized members of its staff. Ongoing Authorization artifacts include monthly TRigger Accountability Log (TRAL), monthly operating system scan results, application scans as directed, updated control allocation table (CAT), and associated memos as directed. All steps in the DHS Mandated tool or System of Record shall be completed correctly, thoroughly and in a timely manner for all steps of the RMF.

D.6. The Contractor shall support the successful remediation of all identified system weaknesses and vulnerabilities that are identified as a result of the aforementioned security review process.

D.7. The Contractor shall submit and analyze monthly operating system vulnerability scans for the DHS Information Security Performance Plan FISMA Scorecard. Vulnerabilities not remediated are generated into Plan of Action and Milestone (POA&Ms) after 30 days.

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 may be disrupted and thus requiring activation of the CP and/or COOP. The contractor's CP/COOP responsibility relates only to the approved system(s) they provide or operate under contract.

E.2. The Contractor shall ensure that contingency plans are consistent with template provided in DHS Mandated System of Record. If access has not been provided initially, the contractor shall use the DHS 4300A, 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 shall test their CP annually and retain records of the annual CP testing for review during periodic audits.

E.6. The Contractor shall record, track, and correct any CP deficiency; any deficiency correction that cannot be accomplished within one month of the annual test shall be elevated to IAD management.

E.7. The Contractor shall ensure the CP addresses emergency response, backup operations, and recovery operations.

E.8. The Contractor shall have an Emergency Response Plan (ERP) that includes procedures appropriate to fire, flood, civil disorder, disaster, bomb threat, or any other man-made or natural incident or activity that may endanger lives, property, or the capability to perform essential functions.

E.9. The Contractor shall have a Backup Operations Plan (BOP) that includes procedures and responsibilities to ensure that essential operations can be continued if normal processing or data communications are interrupted for any reason.

E.10. 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.11. The Contractor shall ensure all TSA data (e.g., email servers, data servers, etc.) is incrementally backed up on a daily basis.

E.12. The Contractor shall ensure a full backup of all network data occurs as required by the system's *availability* security categorization impact rating per the TSA Information Assurance Handbook.

E.13. The Contractor shall ensure all network application assets (e.g., application servers, domain controllers, Information Assurance (IA) tools, etc.) shall be incrementally backed up as required to eliminate loss of critical audit data and allow for restoration and resumption of normal operations within one (1) hour.

E.14. The Contractor shall ensure backup of data to facilitate a full operational recovery within one (1) business day at either the prime operational site or the designated alternate/backup site in accordance with local disaster recovery plan.

E.15. The Contractor shall ensure that data at the secondary location is current as required by the system's *availability* security categorization impact rating.

E.16. 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.17. The Contractor shall adhere to the DHS IT Security Architecture Guidance 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.18. The contractor shall adhere to the DHS IT Security Architecture Guidance for the management of mixed data for OS files, user accounts, externally-accesses data files and audit logs.

F. Program Performance and Audit:

F.1. The Contractor shall comply with requests to be audited and provide responses within three (3) business days to requests for data, information, and analysis from the TSA IAD and management, as directed by the CO.

F.2. The Contractor shall provide support during IAD audit activities and efforts. These audit activities shall include, but are not limited to: requests for system access for penetration testing, vulnerability scanning, incident response and forensic review.

F.3. Upon completion of monthly security scans, findings shall be documented and categorized as High, Moderate, or Low based on their potential impact to the System IT security posture. The
Contractor shall provide TSA with estimates of the total engineering service hours required to support the remediation of open POA&M items. High security findings shall be remediated first in 45 days or less; Moderate security findings shall be remediated in 60 days or less, and Low security findings shall be remediated in 90 days or less. The Contractor shall work with the TSA System Information Systems
Security Officer (ISSO) and the respective CO and/or COR, as well as IAD and the System Owner (as required) to prioritize and plan for the remediation of open POA&Ms. The TSA System ISSO shall maintain all security artifacts and perform Ongoing Authorization (per NIST 800-137 and DHS TSA requirements) and Continuous Diagnostics and Mitigation (CDM) (per OMB M-14-03) activities to ensure active compliance with security requirements. Specific POA&M guidance and information can be found in the SOP 1401 *Plan of Action and Milestone (POA&M) Process*, as well as the DHS 4300A Attachment H *Plan of Action and Milestones (POA&M) Process Guide.*

G. Federal Risk and Authorization Management Program (FedRAMP):

G1. If a vendor is to host a system with an approved Cloud Service Provider (CSP), the CSP and shall adhere to the following:

- Comply with Federal Agency cloud requirements per CCSH;
- Identity and entitlement access management shall be done through Federated Identity;
- SSI, PII and SPII 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 properly cleared and vetted U.S. citizens;
- TSA data shall not leave the United States; and
- The cloud internet connection shall route via an approved DHS Trusted Internet Connection (TIC) 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 with malicious attachments, Uniform Resource Locators and other forms of malware before being delivered to *.gov end-users.

G2. Private Sector System Requirements: TSA shall conduct audits at any time on approved private sector systems, and the system shall be entered into the TSA FISMA Inventory as a system of record (SOR) using the Control Implementation Summary (CIS) provided by the Cloud Service Provider. Security artifacts shall be created and maintained in the DHS Mandated System of Record. The private sector systems are required to go through the Security Authorization Process and the RMF in accordance the Federal Information Systems Management Act (FISMA) and NIST SP 800-37. The cloud internet connection shall be behind a commercial Trusted Internet Connection (TIC) that has E3A deployed.
Security event logs and application logs shall be sent to the TSA SOC. Incidents as defined in the TSA Management Directive 1400.3 Information Technology Security (ITS) and its Attachment 1 (TSA IA 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 and communicated by the COR or contract security point of contact (POC).

H. Information Assurance Policy:

H.1. All proposed services, hardware, software, applications, etc. shall be compliant with applicable DHS 4300A, DHS 4300B (for classified information), TSA MD 1400.3 ITS, TSA IA Handbook, Technical Standards (TSs) and Standard Operating Procedures (SOPs) prior to approval, implementation and operations.

H.2. The contractor solution shall follow all current versions of TSA and DHS policies, procedures, guidelines, and standards, which shall be provided by the CO.

H.3. Authorized access and use of TSA IT systems and resources shall be in accordance with the DHS and TSA information system policies.

I. Data Stored/Processed at Contractor Site:

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

J. Remote Access:

J.1. Any TSA-approved 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 shall be expressly granted, in writing, by the TSA AO.

J.2. Any unauthorized Contractor employee(s) remote access connection to TSA networks shall be terminated immediately at the sole discretion of TSA.

J.3. The Contractor shall use his or her federally issued and approved personal identity verification (PIV) credential/identification badge to access TSA resources to include IT

applications and physical facility.

K. Interconnection Security Agreement (where applicable):

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

K.1. Interconnections between DHS/TSA and non-DHS/TSA 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 using an approved Interagency Agreements (IAA); Memoranda of Understanding/Agreement (MOU/MOA), Service Level Agreements (SLA) or Interconnection Service Agreements (ISA).

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:

This section is not applicable if contract already addresses this clause *DHS Sensitive Information Required Special Contract Terms (MARCH 2015), SAFEGUARDING OF SENSITIVE INFORMATION* for contractsthat have a high risk of unauthorized access to or disclosure of sensitive information.

L.1. The contractor shall satisfy requirements to work with and safeguard Sensitive Security Information (SSI), Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). All support personnel shall understand and rigorously follow DHS and TSA requirements, SSI Policies and Procedures Handbook, and Privacy policies, and procedures for safeguarding SSI, PII and SPII.

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, SPII, SSI, NSS, Sensitive But Unclassified (SBU), and Critical Infrastructure Information (CII) shall be protected according to DHS and TSA security policies and mandates.

L.3. TSA shall identify IT systems transmitting any classified/unclassified/SSI information and requiring 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 (or higher)** 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 current DHS 4300A)

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 SPII shall 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 IA Handbook, and applicable Technical Standards and SOPs.

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

L.7. The Contractor shall ensure all source code is protected from unauthorized access, alterations or dissemination (see TSA IA Handbook, Technical Standard).

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 signed certifications that all assets containing or used to process TSA information have been sanitized in accordance with the TSA MD 1400.3 ITS, TSA IA Handbook, Technical Standards and SOPs. The contractor shall certify in writing that sanitization or destruction has been performed. Sanitization and destruction methods are outlined in the NIST Special Publication 800-88 Guidelines for Media Sanitization, TSA Technical Standard 046 *IT Media Sanitization and Disposition*, and SOP 1400-503 *IT Media Sanitization*. The contractor shall email TSA, PM, CO and COR a signed certification by the contractor's designated senior security officer or senior official, signed proof of sanitization. In addition, the contractor shall provide the TSA CO a master asset inventory list that reflects all assets, government furnished equipment (GFE) or authorized non- GFE that were used to process and store TSA information.

N. Special Considerations and Circumstances (where applicable):

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 shall provide, implement, and maintain a Security Program Plan (SPP) based on the templates provided by the TSA IAD. This plan shall describe the processes and procedures that shall be followed to ensure the appropriate security of IT resources 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). Security controls contained in the plan shall meet the requirements listed in the TSA IA Handbook, Technical Standards and the DHS 4300A (or DHS 4300B for classified information).

N.2 The SPP shall be a living document. It shall be reviewed and updated semi-annually, beginning on the effective date of the contract, to address new processes, procedures, technical or federally mandated security controls and other contract requirement modifications or additions 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 details the approach contained in the offeror's proposal or quote that resulted in the award of this contract and in compliance with the system security requirements.

N.4 The SPP, as submitted to the CO, and accepted by the ISSO, shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

O. Trusted Internet Connection (TIC) Requirements for Managed Trusted Internet Protocol Service Offering (MTIPS):

O.1 MTIPS providers shall comply with the current FedRAMP TIC Overlay requirements in addition to the basic requirements outlined in the current DHS TIC Reference Architecture.

P. ISSO Support:

P.1 The contractor Program Manager shall ensure that contractor ISSO duties and responsibilities align with the TSA IAD/Governance, Risk, and Compliance (GRC) Branch mission and security responsibilities.

Q. Continuous Diagnostics and Mitigation:

Q.1 The Government, through a Continuous Monitoring as a Service (CMaaS) vendor, shall provide the contractor with GFE appliances and tools to support the implementation and maintenance of the Continuous Diagnostics and Mitigation (CDM) Solution. The tools shall be hosted on the DHS' Infrastructure as a Service (IaaS) program. The Government, through the CMaaS vendor, shall provide sensor kits, appliances, probes, and agents that shall be deployed on all contractor Information Systems supporting the TSA.

Q.2 The contractor shall support the installation (including rack and configuration) of sensor kits, appliances, probes and agents on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards.

Q.3 The contractor shall configure/tune their existing endpoint security products to coexist with the identified products to ensure smooth and cohesive functionalities. Credentials (service accounts) shall be provided by the TSA CISO, or designee, for vulnerability scans and host interrogation.

Q.4 The Government, through the CMaaS vendor, shall provide the following support for operations and maintenance of the CDM solution sensor kits:

- Patching (Controlled through a CMaaS Windows Server Update Service (WSUS))
- Hardware troubleshooting & Risk Management (RMA)
- Application maintenance (done from the Government/TSA Management Enclave)
- Vulnerability scanning

Q.5 The contractor shall install TSA-provided CDM Solution patches within two (2) days of issuance, or as directed by TSA, and provide evidence of implementation to the TSA ISSO.

Q.6 The TSA CO (as approved and on behalf of the SO and TSA senior leadership) is authorized to provide technical direction to the contractor for the sole purpose of implementing the CDM Solution. If the technical direction results in any cost incurred by the contractor, for which the contractor shall seek reimbursement from the Government, the contractor shall identify the following information in any cost/price proposal to the Government: name of system owner, summary of the technical direction, date of the technical direction, purpose of the technical direction, summary of actions taken by the contractor, any other information the CO may require to further guide the directed change. The contactor shall receive approval from the CO of the directed and approved change prior to incurring costs associated with the technical direction.

R. Software Guidance:

The CO shall provide a listing of all TSA approved security software upon contract award. The approved security software listing is maintained by the IAD.

R.1 In support of the CDM objective to protect high value assets (HVAs) and information, the Government has acquired security tools in order to conduct Indicator of Compromise (IOC) scans within the mandated time frame. The Government shall provide the tool license and/or equipment for installation of tool agents on all TSA supported assets.

R.2 The contractor shall support efforts to allow for the IOC scanning mandate. This may include installation of tool servers and/or agents within each system's environment and on all TSA supported assets. The Government shall provide the contractor with the tool server(s) that shall not belong to the contractor's system boundary. The tool server shall be reachable from OneNet/TSANet over the Internet. The tool server(s) shall be properly configured to reach all assets with the tool agent installed on the network. Credentials (service accounts) shall be provided for IOC scans and tool interrogation.

R.3 The contractor shall support or perform the installation of forensic software servlet agents on supported Operating Systems on all TSA contract supported devices and environments per TSA engineering, security, and configuration standards. The contractor shall test and upgrade the servlet agents as directed by the IAD.

R.4 The Government shall provide the contractor with a forensic software server that shall not belong to the contractor's system boundary. The contractor shall support or perform the installation of the server. The server shall be reachable from TSANet over the Internet and shall be primarily used for authentication and proxy functions. The server shall be properly configured to reach all assets with the agent installed on the network.

R.5 The contractor shall support efforts of incident response and forensic investigation. This includes authorization to connect TSA authorized equipment where the forensic software servlet agents are reachable to perform analysis.

R.6 The contractor shall install TSA-provided solution patches within two (2) days of issuance, or as directed by TSA CIO, and provide evidence of implementation to the TSA ISSO.

S. Passwords/PINs shall use TSA Approved Multi-factor Authentication (MFA):

S.1 The contract ISSO shall determine and enforce the appropriate frequency for changing passwords/PINs in accordance with appropriate guidance documentation along with the use of a second factor authentication to be in compliance with Executive Order 14028 "Improving the Nation's Cybersecurity" for Multi-factor Authentication (MFA). In the absence of specific guidance documentation, where applicable, passwords shall not remain in effect longer than ninety (90) days.

T. Personal Identity Verification (PIV):

T.1 The Contractor shall use PIV credential/identification badges as the primary means to access TSA resources to include IT applications and physical facility. TSA network domain user account password expiration function shall be disabled when using PIV Machine Based Enforcement (MBE). PINs for PIV card-enabled users shall not expire, and shall have a minimum six-digit PIN when logging into the network using a PIV card.

T.2 The Contractor shall ensure newly developed information system(s) support PIV card authentication. The information system shall be capable to accept and electronically verify PIV credentials.

T.3 The Contractor shall employ information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems.

T.4 The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the approved PIV credentials as the common means of authentication for access to DHS/TSA facilities, networks, and information systems. PIV credentials shall be used as the primary means of authentication for DHS/TSA sensitive IT systems. The Contractor shall use his or her federal issued PIV credentials to access DHS/TSA resources to include IT applications and physical facility.

T.5 The DHS/TSA Security Office shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued PIV credentials/identification cards and building passes that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or any other DHS/TSA-issued cards.

U. End-of-Life (EOL) / End-of-Service (EOS):

U.1 The Contractor shall ensure that any hardware, software or application that is procured develops a full lifecycle plan based on the vendor's established life and service expectancy of the product and total cost of ownership. Any new or existing product that shall reach end-of-life (EOL)* within three (3) years and is part of a TSA FISMA IT System shall require development of a remediation, upgrade, replacement and funding plan to remove the EOL item(s) from the TSA environment completely within that time frame. A plan of action and milestone (POA&M) shall be submitted for risk acceptance to the TSA CISO in order to track remediation milestones appropriately.

*EOL / EOS - Defined as production and/or development, technical support, application updates, spare parts and security patches which are no longer available from the vendor.

V. Maintenance:

V.1 The Contractor shall ensure that the system, once operational, is properly and securely maintained and monitored, to include: immediate response to critical security patches, routine maintenance windows to allow for system updates, and compliance with a defined configuration management process. All patches and system updates shall be properly tested and approved in a development environment ***before*** being implemented in the production environment.

V.2 The contractor shall perform customer support twenty-four (24) hours, seven (7) days a week (i.e., 24/7) within the Continental United States (i.e., CONUS) only.

W. Security in the Agile Development Process (where applicable):

TSA systems shall follow the below guidance when delivering system and application solutions to the agency –

- Applications shall be reviewed prior to acceptance by the Contractor

- Applications shall be assessed, tested and evaluated for Cybersecurity using automated scans, manual testing and compliance with the Cloud Computing Security Requirements Guide and the Application Security and Development STIG
- Contractor shall implement Threat Modeling
- Developer shall deliver a defect list
- Developer shall implement Patching and Configuration Management strategies
- Developer shall use Component Analysis
- Developer shall implement build tests
- Developer shall implement Manual Code Inspection
- Developer shall implement Security Regression Tests
- Developer shall implement Pre-Deployment/Post Deployment Automated Tests
- Developer shall implement industry standard "Every-Sprint Practices", which at a minimum consists of:

    - Threat Modeling
    - Use of Approved Tools
    - Deprecate Unsafe Functions
    - Static Analysis
    - Conduction Final Security Review
    - Certify, Release and Archive

- Developer shall implement industry standard Practices, which at a minimum consists of:

    - Create Quality Gates/Bug Bars
    - Perform Dynamic Analysis
    - Perform Fuzz Testing
    - Conduct Attach Surface Review

- Developer shall implement industry standard One-Time Practices, which at a minimum consists of:

    - Establish Security Requirements
    - Perform Security and Privacy Risk Assessments
    - Establish Design Requirements
    - Perform Attack Surface Analysis
    - Create Incident Response Plan

SECTION IV – FEDERAL ACQUSITION REGULATION (FAR) CLAUSES

1.0 CLAUSES INCORPORATED BY REFERENCE

52.243-1 Changes – Fixed Price, Alt. II (APR 1984)

FAR 52.204-1 APPROVAL OF CONTRACT (DEC 1989)

This contract is subject to the written approval of the Contracting Officer, Susan Mielke, and shall not be binding until so approved.

(End of clause)

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment (Aug 2020)

(a) Definitions. As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Interconnection arrangements means arrangements governing the physical connection of two or more networks to allow the use of another's network to hand off traffic where it is ultimately delivered (e.g., connection of a customer of telephone provider A to a customer of telephone company B) or sharing data and other information resources.

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition.

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment,

system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement.
(1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)