Immigration and Customs Enforcement
Enforcement and Removal Operations
287(g) Program

287(g) Texas Transportation

PROFESSIONAL SUPPORT SERVICES
PERFORMANCE WORK STATEMENT (PWS)

June 2026

Confidentiality Statement

WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel who do not have a valid "need-to-know" without prior approval of an authorized DHS official.

1.0 BACKGROUND

1.0.1 The Enforcement and Removal Operations (ERO) Directorate of U.S. Immigration and Customs Enforcement (ICE) promotes public safety and national security by identifying, arresting, detaining, and removing aliens who undermine the integrity of U.S. immigration laws or pose a danger to communities.

1.0.2 The 287(g) Program, authorized under Section 287(g) of the Immigration and Nationality Act (INA), delegates specific immigration enforcement authority to train and supervise state and local law enforcement officers, (Designated Immigration Officers – DIOs). Texas maintains one of the largest and most active 287(g) programs in the nation, with more than thirteen thousand (13,000) credentialed DIOs.

1.0.3 To maximize the effectiveness of these partnerships and ensure the immediate transfer of custody for removable aliens identified through the program, ERO requires a dedicated, statewide, armed ground transportation capability that provides safe, secure, humane, and expeditious transport services 24 hours per day, 7 days per week, 365 days per year (24/7/365).

1.0.4 These contract transportation services are intended to provide pickup of individuals in the custody of state and local law enforcement partners under 287(g) provisions for immigration related offenses and delivery to ICE ERO offices or designated detention facilities within Texas and to ICE offices or designated detention facilities in the neighboring states of New Mexico and Oklahoma.

1.0.5 This PWS establishes the requirements for a single contractor to provide armed ground transportation services for individuals arrested under the 287(g) Program throughout the State of Texas, with centralized 24/7/365 dispatch operations co-located at the ICE 287(g) National Coordination Center in the greater Nashville, Tennessee area.

1.0.6 As the number of 287(g) partners grows, ICE ERO anticipates transportation needs in all 254 Texas counties. Response time is the key performance metric under this contract. The contractor shall staff and deploy a sufficient number of two-person armed transport teams in Texas to achieve a statewide average response time of 30 minutes or less from dispatch notification to arrival at the pickup location, as calculated on a monthly basis.

2.0 SCOPE OF WORK

2.0.1 The contractor shall provide all management, supervision, personnel, training, certifications, equipment, vehicles, facilities (except space for the dispatch center in the 287(g) National Coordination Center), materials, supplies, and quality control necessary to perform safe, secure, humane, and expeditious armed ground transportation services for individuals placed into ICE custody under the 287(g) Program.

2.0.2 Services shall be provided from any location within the state of Texas and shall include transportation to ICE designated locations, including facilities in Oklahoma and New Mexico, when directed.

2.0.3 Services shall be performed 24 hours per day, 7 days per week, 365 days per year (24/7/365), including all federal holidays and during any periods of lapsed appropriations, with no exceptions.

2.0.4 The Government shall not exercise supervision or control over the contractor's performance of the services described herein. The contractor's personnel shall remain accountable solely to the contractor, who, in turn, is responsible to the Government for ensuring that all tasks are performed in accordance with the requirements of this PWS.

2.0.5 Services are intended for transportation of detainees from state, local, tribal, and other 287(g) partners into ICE custody. However, transportation requests may also include transfers between ICE facilities or from other federal partners to ICE facilities based upon ICE operational needs.

2.0.6 While transportation services are intended for all of Texas within the 120-day transition period, initially the highest priority areas will be the counties in and around the following metro areas and should be operationalized immediately (within 30 days): Dallas-Fort Worth, San Antonio, and Houston.

2.0.7 The transportation services provided in this contract should be scalable in order to accommodate any future contracts or contract amendments, such that the size and scope can be reduced to a smaller footprint in Texas or a footprint that can be expanded beyond Texas and into other states/regions.

2.1 PERIOD OF PERFORMANCE

2.1.1 The proposed period of performance is four years, structured as:

2.1.2 Base Period: 12 months (includes 120-day transition in).

2.1.3 Option Period: 36 months.

2.2 PLACE OF PERFORMANCE

2.2.1 Primary place of performance: State of Texas (all 254 counties).

2.2.2 Delivery locations: ICE or ICE designated facilities in Texas, Oklahoma, and New Mexico, as directed.

2.2.3 Dispatch Center: Space will be available within the ICE 287(g) National Coordination Center in the greater Nashville, Tennessee area. This Coordination Center is in the planning stages and is projected to become operational in 2026.

2.3 TELEWORK ELIGIBILITY

2.3.1 Telework eligibility under this contract: None.

2.4 HOURS OF WORK

2.4.1 The contractor shall ensure adequate staffing coverage to meet operational requirements 24 hours per day, 7 days per week, 365 days per year (24/7/365).

2.4.2 The transportation and dispatch mission is critical law enforcement support and is exempt from planned and unplanned Government closures, including shutdowns due to lapses in funding.

2.4.3 The contractor shall remain flexible in allocating staffing resources to address fluctuations in transport volume.

2.4.4 Overtime shall not be authorized under this contract unless expressly approved in advance, in writing, by the COR.

3.0 REFERENCES AND APPLICABLE DOCUMENTS

3.0.1 The contractor shall comply with all applicable laws, regulations, policies, and standards, including but not limited to the following:

3.0.1.1 Immigration and Nationality Act § 287(g).
3.0.1.2 National Detention Standards (NDS) 2026.
3.0.1.3 ICE Family Residential Standards (latest version).
3.0.1.4 Prison Rape Elimination Act (PREA) Standards – 28 CFR Part 115.
3.0.1.5 DHS Instruction 121-01-007-02 – The DHS Personnel Suitability and Security Program (or latest revision).
3.0.1.6 DHS Sensitive Systems Policy Directive 4300A.
3.0.1.7 Federal Acquisition Regulation (FAR) DHS Class Deviation 25-28 for Part 46 – Quality Assurance.
3.0.1.8 Federal Motor Carrier Safety Regulations (49 CFR Parts 390–399).
3.0.1.9 OSHA Bloodborne Pathogens Standard (29 CFR 1910.1030).
3.0.1.10 ICE Use of Force Policy (latest version).
3.0.1.11 ICE National Detention Standards 2025.

3.0.2 The contractor shall comply with all subsequent updates and revisions to the authorities and standards listed in Section 3.0.

4.0 DEFINITIONS AND ACRONYMS

4.0.1 For the purposes of this PWS, the following definitions and acronyms apply:

4.0.1.1 **287(g) Partner** – A state or local law enforcement agency with an active Memorandum of Agreement under § 287(g) of the Immigration and Nationality Act (INA).

4.0.1.2 **Designated Immigration Officer (DIO)** – A state or local law enforcement officer trained and credentialed by ICE to perform limited immigration enforcement functions.

4.0.1.3 **Detainee/Alien** – Any individual in ICE custody under the authority of the 287(g) Program.

4.0.1.4 **Transport Team** – A minimum of two (2) armed, cross trained personnel consisting of one driver and one guard.

4.0.1.5 **Response Time** – The elapsed time from dispatch notification to arrival at the pickup location; shall not exceed a statewide average of thirty (30) minutes.

4.0.1.6 **Armed** – Carrying an approved duty firearm with a chambered round and the required spare magazines.

4.0.1.7 **Form G-391** – ICE Request for Transport / Detailed Manifest.

5.0 PERFORMANCE REQUIREMENTS AND MINIMUM STANDARDS

5.0.1 The contractor shall perform the seven primary task areas described in this section to meet the minimum required output for this contract. These task areas define the core services necessary for the successful execution of statewide 287(g) armed ground transportation operations.

5.0.2 While the minimum requirements are clearly stated, additional activities within the scope of this PWS may be required to ensure comprehensive mission support and operational success.

5.1 TASK 1 – STATEWIDE ARMED TRANSPORT OPERATIONS

5.1.1 The contractor shall provide safe, secure, humane, and expeditious armed ground transportation services for individuals being transferred from 287(g) partner agencies to ICE custody.

5.1.2 Each transport shall be conducted by a minimum two-person armed team (one driver and one guard), both cross-trained and capable of performing either role.

5.1.3 All detainees shall be thoroughly searched, restrained in accordance with NDS 2026, and seated in the secure compartment prior to movement.

5.1.4 Detainees shall remain under constant visual and/or video observation by at least one-armed team member at all times while outside a secure facility.

5.1.5 The contractor shall ensure humane treatment at all times, including maintaining appropriate climate control within transport vehicles.

5.1.6 The contractor shall prevent unauthorized communication between detainees and the public and shall immediately report any attempted or successful escape, disturbance, or medical emergency to ICE in accordance with established procedures.

5.1.7 **Deliverable:** Demonstrated 100 percent compliance with transport requirements, verified through daily operational reports and random Government audits.

5.2 TASK 2 – GEOGRAPHIC COVERAGE AND 30-MINUTE RESPONSE CAPABILITY

5.2.1 The contractor shall maintain, at all times, a sufficient number of two-person armed transport teams to achieve a 30-minute statewide average response time to 287(g) transport requests anywhere in Texas.

5.2.2 Loiter (staging) locations used while awaiting transport requests shall be within the state of Texas and shall be identified, managed, and adjusted as needed by the contractor.

5.2.3 The maximum allowable response time is 30 minutes from dispatch notification to on scene arrival at the pickup location, measured as a statewide average on a monthly basis. Individual transport requests or requests within an individual county may exceed or fall below 30 minutes; however, the calculated statewide average shall not exceed 30 minutes.

5.2.4 Response time performance shall be calculated on a monthly basis and shall reset at the beginning of each month.

5.2.5 The contractor shall continuously monitor demand and dynamically adjust the staging and deployment of transport teams to ensure compliance with the statewide 30-minute average response requirement.

5.2.6 The 30-minute response time requirement begins with centralized dispatch communication and notification to the transport team and ends at transport team's arrival at the pickup location. There is no contractual time standard for delivery of detainees to the receiving facility after pickup.

5.2.7 Based on operational needs and existing trends, ICE ERO may conduct surge operations in specific geographic areas that result in increased transport requests during defined periods. The contractor shall plan for and support such surge operations while maintaining compliance with response time requirements to the maximum extent practicable.

5.2.8 **Deliverable:** Daily Operational Report providing key details of all requests for transport, including request time, dispatch time, arrival time, calculated response time, pickup and delivery locations, and any response time- exceptions. 100 percent compliance.

5.3 TASK 3 – 24/7/365 CENTRALIZED DISPATCH OPERATIONS

5.3.1 The contractor shall establish and continuously operate a centralized dispatch center serving as the single command and control location for all contract transportation operations. The dispatch center shall be physically located- within the ICE 287(g) National Coordination Center in the greater Nashville, Tennessee area.

5.3.2 The dispatch center shall be staffed, at a minimum, with two fully trained dispatchers and one supervisor on duty at all times (24/7/365).

5.3.3 The dispatch center shall maintain:

a. Direct voice communication with every field team;
b. Realtime GPS tracking of all transport vehicles;
c. Capability to electronically generate, transmit, and receive Form G-391; and
d. Develop and host a secure website which houses and displays all key operational data in real time or near real time. ICE personnel shall have access to view the website and download data.

5.3.4 Upon receipt of a transport request, dispatch personnel shall:

a. Verify the identity and credentials of the caller;
b. Confirm or determine the appropriate delivery location with on duty ICE ERO personnel at the National Coordination Center or a local ICE ERO office, or ICE representatives, as applicable;
c. Dispatch the nearest appropriate transport team;
d. Electronically transmit Form G-391 to the assigned transport team; and
e. Maintain continuous tracking and communication with the transport team until delivery is acknowledged by the receiving ICE officer or facility.

5.3.5 The contractor shall maintain an electronic master log of every transport request and completed transport. At a minimum, the log shall include date and time of request, requesting agency, pickup and delivery locations, assigned team, timestamps (dispatch, arrival, departure, and delivery), and any notable incidents.

5.3.6 For each transport request, the contractor shall coordinate with local ICE field offices, sub-offices near the designated transport request location, or ICE representatives at the National Coordination Center to confirm and document the designated delivery/end point.

5.3.7 **Deliverable:** Daily Dispatch Performance Report documenting, at a minimum, call volume, system uptime, response time- metrics, pickup and delivery locations, and identity/number of subjects transported.

5.4 TASK 4 – SECURE WEBSITE OF OPERATIONS

5.4.1 The contractor shall create, host, and allow access to ICE personnel a secure website which contains key operational data related to transportation operations (requests for transport, response time, individuals transported, delivery location, transport teams involved, incidents, etc).

The secure website shall store only the minimum data elements necessary to support transportation operations. This may include detainee name, Alien Number (A number), and date of birth as reflected on Form G-391, together with associated transport information such as pickup and delivery locations, dates and times, and incident details. No biometric data or classified information shall be stored in the secure website.

5.4.2 The secure website is intended to be an operational dashboard which allows both the contractor and ICE to maintain the highest levels of situational awareness. The website also serves as a historic record of operations with the ability to search and download data.

5.4.3 The secure website is a stand-alone, contractor-hosted website that does not connect to or integrate with any Government information system. ICE personnel will access the site via standard web browsers over encrypted connections to view and download data. The website will be used exclusively to support performance of this contract and will handle Controlled Unclassified Information (CUI), including law enforcement sensitive data and PII/SPII, in accordance with applicable DHS and ICE requirements.

5.4.4 **Deliverable:** Daily audit of the secure portal verified through daily access and random Government audits.

5.5 TASK 5 – USE OF ICE FORM G391 OR EQUIVALENT (CHAIN OF CUSTODY DOCUMENTATION)

5.5.1 Form G-391 shall be generated and electronically transmitted from the central dispatch center to the assigned transport team for each detainee transport.

5.5.2 Form G-391 shall be completed for every detainee, shall include all required data fields, and shall be electronically signed by the receiving ICE officer. The completed form shall be uploaded to the secure portal within fifteen (15) minutes of delivery.

5.5.3 The contractor shall ensure 100 percent completion, accuracy, and timely submission of all Form G391 documents, and shall implement internal quality controls to promptly identify- and correct any deficiencies.

5.5.4 **Deliverable:** Daily audit of the secure portal confirming 100 percent compliance with Form G-391 completion, accuracy, and upload requirements.

5.6 TASK 6 – VEHICLE STANDARDS, MAINTENANCE, SANITATION, AND OPERATIONAL READINESS

5.6.1 All transport vehicles used under this contract shall be current model full---size vans or large SUVs equipped with:

a. A minimum secure capacity of four (4) detainees; and
b. A full steel security partition separating detainees from staff.

5.6.2 The contractor shall maintain an average monthly fleet operational readiness rate of at least eighty percent (≥80 percent), defined as vehicles fully mission capable- and available for assignment.

5.6.3 After every transport, vehicles shall be cleaned and disinfected in accordance with current CDC guidelines and any applicable ICE policies or directives.

5.6.4 The contractor shall maintain electronic records of all preventive and corrective maintenance, sanitation events, and pre and post- trip- inspections for each vehicle, and shall make such records available to the COR upon request.

5.6.5 **Deliverable:** Monthly Fleet Readiness and Sanitation Report, including fleet status (operational, down for maintenance, or out of service), summary of maintenance actions, and sanitation/inspection logs.

5.7 TASK 7 – FIREARMS, AMMUNITION, AND ARMING PROTOCOLS

5.7.1 Duty firearms carried by contractor personnel under this contract shall be standardized or uniform 9mm handguns.

5.7.2 Ammunition shall be factory loaded hollow- point ammunition, replaced at least annually, and stored in climate-controlled armories or secure storage consistent with applicable law and ICE policy.

5.7.3 Each armed officer shall, at a minimum, carry:

a. One duty pistol (with a chambered round) and two spare magazines;
b. A Level III (or higher) retention holster;

5.7.4 The contractor shall maintain daily firearms accountability logs, reconciled with dispatch records at each shift change. Any discrepancies, losses, or suspected thefts shall be reported to the COR and appropriate law- enforcement within one (1) hour of discovery.

5.7.5 All armed personnel shall successfully complete firearms qualification at least annually, using a course of fire administered by a state certified or nationally- certified firearms instructor, and shall maintain documentation of such qualification.

5.7.6 **Deliverable:** Monthly arming compliance and qualification status report, submitted via the secure portal, documenting firearms inventories, accountability results, and current qualification status for each armed employee.

6.0 SECURITY AND SUITABILITY REQUIREMENTS

6.0.1 The contractor shall comply with all Department of Homeland Security (DHS) and U.S. Immigration and Customs Enforcement (ICE) security policies, directives, and standards in effect at the time of award and as updated during contract performance.

6.0.2 All positions under this contract are designated as high risk public trust positions in accordance with- 5 CFR Parts 731 and 1400 and DHS Instruction 121-01-007-02, *The DHS Personnel Suitability and Security Program* (or latest revision).

6.0.3 The contractor shall safeguard all CUI, including PII and Sensitive PII, processed or stored in contractor systems under this contract, including the secure web portal described in Section 13.0, in accordance with HSAR 3052.204-72, HSAR 3052.204-73 if incorporated in the contract, and applicable DHS and ICE policies.

6.1 POSITION RISK AND SENSITIVITY DESIGNATION

6.1.1 Every contractor and subcontractor employee who will have direct contact with detainees; operate transport vehicles; carry firearms; access ICE systems, facilities, or secure areas; or handle Personally Identifiable Information (PII), Alien Numbers (A numbers), or criminal history information shall be designated as High Risk-Public Trust.

6.1.2 No individual may begin performance of any kind under this contract, including training or onboarding activities, until the Government has completed a favorable suitability determination and issued written Entry on Duty (EOD) authorization.

6.2 PERSONNEL SECURITY VETTING REQUIREMENTS

GENERAL

The United States Immigration and Customs Enforcement (ICE) has determined that performance of the tasks as described in this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

PRELIMINARY FITNESS DETERMINATION

ICE will exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for contractor applicants/employees, based upon the results of a Fitness screening process. ICE may, as it

deems appropriate, authorize and make a favorable expedited preliminary Fitness determination based on preliminary security checks. The preliminary Fitness determination will allow the contractor employee to commence work temporarily prior to the completion of a Full Field Background Investigation. The granting of a favorable preliminary Fitness shall not be considered as assurance that a favorable final Fitness determination will follow as a result thereof. The granting of preliminary Fitness or final Fitness shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by ICE, at any time during the term of the contract. No employee of the contractor shall be allowed to enter on duty and/or access sensitive information or systems without a favorable preliminary Fitness determination by the Office of Professional Responsibility (OPR), ICE Personnel Security Division (PSD). No employee of the contractor shall be allowed unescorted access to a Government facility without a favorable preliminary Fitness determination by OPR PSD. Contract employees are processed in accordance with 5 CFR 731, and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, those having direct contact with Detainees will also have 6 CFR § 115.117 considerations made as part of the Fitness screening process. Sexual Abuse and Assault Prevention Standards implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003)).

CONTRACTOR EMPLOYEE FITNESS SCREENING

Screening criteria under 5 CFR 731, and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, that may exclude contractor employees from consideration to perform under this agreement includes:

- Misconduct or negligence in employment;
- Criminal conduct;
- Material, intentional false statement or deception of fraud in examination or appointment;
- Dishonest conduct;
- Excessive alcohol use, without evidence of rehabilitation, of a nature and duration that suggests that the applicant or appointee would be prevented from performing the duties of the position in question, or would constitute a direct threat to the property or safety of the applicant or appointee or others;
- Illegal use of narcotics, drugs, or other controlled substances, without evidence of substantial rehabilitation;
- Knowing and willful engagement in acts or activities designed to overthrow the U.S. Government by force;
- Any statutory or regulatory bar which prevents the lawful employment of the person involved in the position in question (for Excepted Service employees);
- Violent conduct; and
- Any other nondiscriminatory reason that an individual's employment (or work on a contract) would not protect the integrity or promote the efficiency of the service.

Screening criteria under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards) implemented pursuant to Public Law 108-79 (Prison Rape Elimination Act (PREA) of 2003) or successor thereto, that WILL exclude contractor employees from consideration to perform under this agreement includes:

- Engaged in Sexual Abuse in a Prison, Jail, Holding Facility, Community Confinement Facility, Juvenile Facility, or other Institution as defined under 42 USC 1997;
- Convicted of engaging or attempting to engage in sexual activity facilitated by force, overt or implied threats of force, or coercion, or if the victim did not consent or was unable to consent or refuse;
- Civilly or administratively adjudicated to have in engaged in such activity.

Subject to existing law, regulations and/or other provisions of this Agreement, undocumented noncitizens shall not be employed by the contractor.

POSITION DESIGNATION

In accordance with 5 CFR part 731, and 5 CFR 1400. Agencies are required to designate position risk and sensitivity level for all contractor employees to determine the commensurate level of background investigation. The public trust risk of a position is the assessment of the degree of potential damage to the efficiency or integrity of the service that could arise from misconduct by the incumbent in the position.

Therefore, once the contract is awarded and before the vendor starts submitting personnel for security vetting, the contractor will provide, through the Contracting Officer's Representatives (CORs) a list of all positions, to include titles and specific description of the duties for each of positions assigned to support the contract.

BACKGROUND INVESTIGATIONS

Contractor employees (to include applicants, temporary, part-time and replacement employees) under the contract, needing access to sensitive information and/or ICE Detainees, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through OPR PSD. Contractor applicant/employees are nominated by a Contracting Officer Representative (COR) for consideration to support this contract via submission of the DHS Form 11000-25 and ICE Supplement to the DHS Form 11000-25 to OPR PSD. This contract shall submit the following security vetting documentation to OPR PSD, through the COR, within 10 days of notification of initiation of an Electronic Application for Background Investigations (eAPP), in the automated on-line system:

1. Standard Form 85P (Standard Form 85PS (with supplement to 85P required for those with direct contact with detainees or armed positions)), "Questionnaire for Public Trust Positions" or successor thereto form completed online and archived by the contractor applicant/employee in their eAPP account.

2. Signature Release Forms (Three total) generated by eAPP upon completion of Questionnaire (e-signature recommended/acceptable). Completed online and archived by the contractor applicant/employee in their eAPP account.

3. Electronic fingerprints taken at an approved facility **OR** two (2) SF 87 Fingerprint Cards (current revision) sent to OPR PSD. Additional information regarding fingerprints will be sent to the contractor applicant/employee from OPR PSD.

4. Optional Form 306 Declaration for Federal Employment. This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

5. Social Security Administration 89 form (SSA-89): Authorization for the Social Security Administration (SSA) to Release Social Security Number (SSN) Verification, which requires a hard signature from the applicant. This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

6. If occupying PREA designated position: Questionnaire regarding conduct defined under 6 CFR § 115.117 (Sexual Abuse and Assault Prevention Standards). This document is sent as an attachment in an e-mail to the contractor applicant/employee from OPR PSD.

7. One additional document may be applicable if the contractor applicant/employee was born abroad. If applicable, the document will be sent as an attachment in an e-mail to OPR PSD from the contractor applicant/employee.

Contracting companies with 300 or more personnel will be required to initiate their own personnel security questionnaires (eAPP) via the DCSA/NBIS portal. OPR PSD will provide training to contractor personnel on how to initiate their applicant's security documents prior to submission to PSD for security vetting.

Contractor employees who have an adequate, current investigation by another Federal Agency may not be required to submit complete security packages; the investigation may be accepted under transfer of trust. The questionnaire related to 6 CFR § 115.117 listed above in item 5 will be required for positions designated under PREA. OPR PSD will determine if personnel meet transfer of trust requirements at the initial stage of processing and prior to requesting a new security questionnaire.

Required information for submission of security packet will be provided by OPR PSD at the time of award of the contract. Only complete packages will be accepted by OPR PSD as notified by the COR.

To ensure adequate background investigative coverage, contractor applicants/employees must currently reside in the United States or its Territories. Additionally, contractor applicants/employees are required to have resided within the United States or its Territories for three or more years out of the last five (ICE retains the right to deem a contractor applicant/employee ineligible due to insufficient background coverage). This timeline is assessed based on the signature date of the standard form questionnaire submitted for the applied position. Contractor employees falling under the following situations may be exempt from the residency requirement: 1) work or worked for the U.S. Government in foreign countries in federal civilian or military capacities; 2) were or are dependents accompanying a federal civilian or a military employee serving in foreign countries so long as they were or are authorized by the U.S.

Government to accompany their federal civilian or military sponsor in the foreign location; 3) worked as a contractor employee, volunteer, consultant or intern on behalf of the federal government overseas, where stateside coverage can be obtained to complete the background investigation; 4) studied abroad at a U.S. affiliated college or university; or 5) have a current and adequate background investigation (commensurate with the position risk/sensitivity levels) completed for a federal or contractor employee position, barring any break in federal employment or federal sponsorship.

Only U.S. citizens and Legal Permanent Residents are eligible for employment on contracts requiring access to DHS sensitive information unless an exception is granted as outlined under DHS Instruction 121-01-007, Revision 2, dated August 10, 2024. Per DHS Sensitive Systems Policy Directive 4300A, only U.S. citizens are eligible for positions requiring access to DHS Information Technology (IT) systems or positions that are involved in the development, operation, management, or maintenance of DHS IT systems, unless an exception is granted as outlined under DHS Instruction 121-01-007, Revision 2, dated August 10, 2024.

CONTINUED ELIGIBILITY

ICE will exercise full control over granting, denying and/or restrict facility and information access of any contractor employee whose actions conflict with Fitness standards contained in 5 CFR 731 and DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, or who violate standards of conduct under 6 CFR § 115.117. The Contracting Officer or their representative can determine if a risk of compromising sensitive Government information exists or if the efficiency of service is at risk and may direct immediate removal of a contractor employee from contract support.

The Federal Government is transitioning to Trusted Workforce (TW) 2.0, which is a government-wide reform effort overhauling the personnel vetting process. One of the principles of this transition is eliminating the traditional five-year periodic reinvestigation requirements, and enrolling personnel into continuous vetting programs. All contractor employees will be subjected to the transition and will be enrolled into a continuous vetting system at a date to be determined. Continuous vetting will replace the traditional five-year periodic background investigation, allowing for background investigations to be conducted if/when derogatory information is discovered.

Enrollment will include multiple requirements from all personnel and potential changes to processes, procedures, and systems. This contract will comply with all requirements that facilitate the mandated transition to TW 2.0.

OPR PSD will evaluate concerns received via multiple sources under the continuous vetting process, to evaluate continued Fitness of contractor employees. If concerns cannot be mitigated, the contractor will be removed from the ICE contract upon notification from OPR PSD.

REQUIRED REPORTS AND REPORTING REQUIREMENTS

The contractor will notify OPR PSD, via the COR providing an ICE Form 50-005, Contractor Employee Separation Clearance Checklist, of all terminations/resignations of contractor employees under the contract within five days of occurrence to the

ICEDepartureNotification@ice.dhs.gov group box. The contractor will return any expired ICE issued identification cards and building passes of terminated/resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

IAW DHS Instruction 121-01-007, Revision 2, dated August 10, 2024, the Contracting Officer's Representatives (CORs) notify the servicing personnel and industrial security offices when a contractor employee is no longer working for ICE.

The contractor is required to report any derogatory information concerning the individual immediately, in accordance with the contract requirements.

The contractor will report any adverse information coming to their attention concerning contractor employees under the contract to OPR PSD, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report should include the contractor employees' full name and social security number, along with the adverse information being reported. See Contractor Employee Fitness Screening section, screening criteria for reportable issues. Report this information to PSD-CEP-REPORTING@ice.dhs.gov.

The contractor will provide, through the COR, a Quarterly Report (on a Microsoft Excel Spreadsheet) containing the names of contractor employees who are actively serving on their contract. The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy. This list is what ICE Industrial Security uses to reconcile the contract quarterly.

CORs will submit reports to PSD-Industrial-Security@ice.dhs.gov no later than the 10th day of each January, April, July and October.

Contractors, who are involved with management and/or use of information/data deemed "sensitive" to include 'law enforcement sensitive" are required to complete the DHS Form 11000-6-Sensitive but Unclassified Information Non-Disclosure Agreement (NDA) for contractor employee access to sensitive information. The NDA will be administered by the COR to all contract personnel within 10 calendar days of the entry on duty date. The completed form shall remain on file with the COR for purpose of administration and inspection.

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information

because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, *DHS Policy for Sensitive Information* and ICE Policy 4003, *Safeguarding Law Enforcement Sensitive Information*.

DHS Management Directive 11042.1, *DHS Policy for Sensitive Information*: https://www.dhs.gov/sites/default/files/publications/Management%20Directive%2011042.1%20Safeguarding%20Sensitive%20But%20Unclassified%20%28For%20Official%20Use%20Only%2 9%20Information_0.pdf;

ICE Policy 4003, *Safeguarding Law Enforcement Sensitive Information*: https://www.ice.gov/node/64612

Any unauthorized disclosure of information should be reported to ICE.ADSEC@ice.dhs.gov.

6.3 SECURITY MANAGEMENT

The contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with OPR PSD through the COR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the contractor.

The COR and OPR shall have the right to inspect the procedures, methods, and facilities utilized by the contractor in complying with the security requirements under this contract. Should the COR determine that the contractor is not complying with the security requirements of this contract, the contractor will be informed in writing by the Contracting Officer of the proper action to be taken to effect compliance with such requirements.

6.4 INFORMATION TECHNOLOGY SECURITY

When sensitive government information is processed on Department telecommunications and automated information systems, the contract company agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS MD 4300.1*, Information Technology Systems Security* (or its replacement).

Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractor employees who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, regardless of if the failure results

in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

6.5 INFORMATION SYSTEMS SECURITY TRAINING AND OVERSIGHT

In accordance with Office of the Chief Information Officer (OCIO) requirements and provisions, all contractor employees accessing Department IT systems or processing DHS sensitive data via an IT system will require an ICE issued/provisioned Personal Identity Verification (PIV) card. Additionally, Cybersecurity Awareness Training (CSAT) will be required upon initial access and annually thereafter. CSAT training will be provided by the appropriate component agency of DHS.

Contractor employees, who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices, systems rules of behavior, to include Unauthorized Disclosure Training, available on the ICE Training System (ITS) or by contacting ICE.ADSEC@ice.dhs.gov. Contractor employees with significant security responsibilities shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. System Administrators should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

6.6 SECURITY INCIDENTS AND REPORTING

6.6.1 The contractor shall immediately take appropriate action to contain, mitigate, and document any actual or suspected security incident, including but not limited to:

a. Loss, theft, or compromise of PII, Sensitive Security Information (SSI), or other sensitive data.
b. Unauthorized access to, or disclosure of, DHS or ICE information.
c. Loss or compromise of access credentials, badges, tokens, or authentication devices.
d. Any suspected or confirmed cyber incident affecting systems used to process, transmit, or store Government information.

6.6.2 The contractor shall report any such incident to the COR and the ICE Office of Professional Responsibility (or other designated point of contact) within one (1) hour of discovery, and shall cooperate fully with any ensuing inquiry, investigation, or forensic activity.

6.6.3 The contractor shall provide written follow-up reports, including root- cause analysis and corrective actions, in the format and within the timeframes- specified by the Government.

6.7 REMOVAL FROM DUTY

6.7.1 The Government may, at its sole discretion, direct the contractor to immediately remove from contract performance any individual who:

a. Fails to maintain a favorable suitability determination or required clearance;
b. Is found to have provided false or misleading information during the screening or reinvestigation process;
c. Violates PREA standards or any applicable DHS/ICE policy;
d. Engages in misconduct, negligence, or behavior inconsistent with the safety, security, or integrity of ICE operations; or
e. Otherwise presents a risk, in the judgment of the Government, to detainees, staff, or mission execution.

6.7.2 Upon notification by the Government, the contractor shall ensure the individual is immediately removed from all duties under this contract and from access to ICE facilities, systems, and information.

6.7.3 The contractor shall notify the COR in writing within four (4) hours of any such removal and shall provide, at no additional cost to the Government, a fully screened and EOD authorized-replacement within ten (10) calendar days, unless otherwise directed by the Government.

6.7.4 Removal of a contractor employee under this section shall not relieve the contractor of its responsibility to meet all contract requirements, including staffing and performance standards.

7.0 PERSONNEL REQUIREMENTS AND KEY PERSONNEL

7.0.1 The contractor shall ensure that all personnel (including subcontractor personnel) assigned to this contract meet the minimum qualifications, professional standards, and training requirements specified in this section.

7.0.2 The contractor shall maintain sufficient staffing levels to meet all operational and performance requirements of this PWS at all times.

7.1 MINIMUM QUALIFICATIONS (ALL PERSONNEL)

7.1.1 Every individual performing work under this contract, including subcontractor personnel, shall meet or exceed the following minimum qualifications:

a. U.S. citizenship or lawful permanent resident status with valid work authorization.
b. Minimum age of eighteen (18) years on date of hire.
c. High school diploma or state accredited- General Educational Development (GED) certificate.
d. Valid driver's license; Class B Commercial Driver's License (CDL) with passenger endorsement is preferred for driving assignments.
e. Fluency in English (read, write, speak, and understand).
f. Ability to qualify with an approved duty pistol in accordance with Section 5.6 and applicable law and policy.
g. Possession of a valid Texas Level III Commissioned Armed Security Officer license (or recognized reciprocal license), obtained no later than sixty (60) days after contract award or date of hire, as applicable.
h. Physical capability to perform required duties, including defensive tactics, detainee control, and operation of vehicles and equipment, with or without reasonable accommodation.

7.1.2 The contractor shall ensure that all personnel maintain required licenses, certifications, and qualifications throughout the period of performance.

7.1.3 The contractor shall promptly remove from contract performance any individual who no longer meets the minimum qualifications or who loses any required license or certification.

7.2 KEY PERSONNEL

7.2.1 The following positions are designated as Key Personnel under this contract:

a. Program Manager.
b. Deputy Program Manager.
c. Operations Manager.
d. Training Manager.
e. Fleet Manager.

7.2.2 The contractor shall designate qualified individuals for each Key Personnel position and shall submit résumés and full background packages for Government review and approval prior to assignment.

7.2.3 Replacement of any Key Personnel shall require prior written approval by the Contracting Officer (CO), in coordination with the Contracting Officer's Representative (COR).

7.2.4 Proposed replacement Key Personnel shall meet or exceed the qualifications and experience of the individual being replaced and shall be fully capable of performing all duties associated with the position.

7.2.5 The contractor shall ensure that each individual serving in a Key Personnel role provides at least thirty (30) calendar days written notice of resignation, to the extent practicable. The contractor shall promptly propose a qualified replacement to avoid gaps in coverage.

7.2.6 The contractor shall ensure continuous coverage of Key Personnel functions and shall not leave any Key Personnel position vacant for more than thirty (30) calendar days without written Government approval.

7.3 UNIFORMS, IDENTIFICATION, GROOMING, AND PROFESSIONAL CONDUCT

7.3.1 Uniform Requirements

7.3.1.1 The contractor shall provide and require the wear of a standardized uniform for all transport and security personnel, which shall include:

a. Tactical -style trousers and polo shirt or Battle Dress Uniform (BDU)-style shirt in navy blue, gray, black, or other subdued color.
b. Clear identification of "TRANSPORT OFFICER" and the company name, embroidered or affixed in a visible location on the shirt or outer garment.
c. Duty belt with approved holster, magazine pouches, and carriers for handcuffs and any other required equipment.
d. Appropriate footwear (closed -toe, supportive, professional in appearance) suitable for armed transport duties.
e. Weather appropriate- outerwear (e.g., jacket or rain gear) that is consistent with the uniform and does not obscure identification.

7.3.2 Identification Requirements

7.3.2.1 The contractor shall issue a photo identification (ID) badge to each employee assigned to this contract.

7.3.2.2 The ID badge shall, at a minimum, display the individual's full name, photograph, company name, unique employee number, and expiration date.

7.3.2.3 The ID badge shall be worn visibly on the outermost garment at all times while on duty, unless specifically exempted for safety or operational reasons by ICE.

7.3.3 Grooming Standards

7.3.3.1 The contractor shall establish and enforce grooming standards that promote a professional and disciplined appearance and support officer safety.

a. Male personnel: Hair shall be neat, clean, and not extend below the top of the collar. Sideburns shall not extend below the bottom of the ear. Facial hair, if worn, shall be neatly trimmed and

generally not exceed one half- (½) inch in length.
b. Female personnel: Hair shall be neat, clean, and secured in a manner that does not interfere with the proper wear of headgear or body armor (if issued) or with the safe performance of duties.
c. Tattoos and body markings: No visible tattoos on the face, neck, or hands shall depict content that is extremist, indecent, or racially or ethnically derogatory. The contractor shall ensure that any such tattoos are appropriately covered while on duty.

7.3.4 Professional Conduct

7.3.4.1 All personnel shall conduct themselves in a professional, courteous, and respectful manner when interacting with detainees, ICE personnel, 287(g) partners, and members of the public.

7.3.4.2 Prohibited conduct (subject to immediate removal from contract performance) includes, but is not limited to:

a. Fraternization or any personal, romantic, or financial relationship with detainees or their family members.
b. Accepting gifts, money, favors, or other items of value from detainees, detainee family members, or representatives.
c. Use of profanity, slurs, or derogatory language directed at detainees, coworkers, or Government personnel.
d. Unauthorized photography, video recording, or audio recording of detainees, ICE operations, or secure areas.
e. Sleeping or inattentiveness while on duty.
f. Use, possession, or influence of alcohol or illegal drugs while on duty or within eight (8) hours prior to reporting for duty.
g. Unauthorized or excessive use of force or failure to report a use of- force incident in accordance with policy.
h. Any form of sexual contact, harassment, or abuse involving detainees, coworkers, or others encountered in the performance of contract duties.

7.3.4.3 The contractor shall ensure that personnel understand their obligation to report any observed or suspected misconduct, including violations of this PWS, ICE policy, or applicable law. Reports shall be made to the Program Manager and the COR as soon as practicable.

7.4 STAFFING CONTINUITY

7.4.1 The contractor shall maintain 100 percent of required staffing levels, including sufficient transport teams to meet performance standards under Section 5.2 throughout the state of Texas.

7.4.2 The contractor shall develop and maintain contingency plans to mitigate the impact of turnover, extended absences, or sudden loss of personnel, including cross training, relief personnel, and surge staffing options.

7.4.3 Replacement of any employee (including non-Key personnel) shall occur within ten (10) calendar days of vacancy, with a fully qualified and EOD- approved- individual, unless otherwise authorized in writing by the COR.

7.4.4 Staffing adjustments, reassignments, or reductions that may impact the contractor's ability to meet contractual performance requirements shall be communicated to the COR in advance, along with a mitigation plan.

8.0 TRAINING AND CERTIFICATION REQUIREMENTS

8.0.1 The contractor shall develop, implement, and maintain a comprehensive training program that ensures all personnel are fully qualified to perform their assigned duties in accordance with this PWS and all applicable DHS/ICE policies and standards.

8.0.2 The contractor's training program shall, at a minimum, meet or exceed the requirements contained in ICE National Detention Standards (NDS) 2026, applicable PREA standards, and any other training requirements specified by ICE for contract personnel.

8.0.3 The contractor shall ensure that no individual performs unsupervised duties under this contract until all required initial training and certifications for that position have been successfully completed and documented.

8.1 INITIAL TRAINING PROGRAM

8.1.1 The contractor shall provide an initial training program for all newly assigned personnel (including subcontractor personnel) of not less than twenty-four (24) hours in duration, unless otherwise approved in writing by the Government.

8.1.2 The initial training program shall be documented in a written curriculum and shall include, at a minimum, the following topics:

a. Overview of DHS and ICE missions, with emphasis on ERO and the 287(g) Program.
b. Legal authorities and limitations relevant to detainee transportation and contractor personnel.
c. Use of- force- policy, continuum, and reporting requirements, consistent with ICE Use of Force Policy.
d. Defensive tactics, detainee control techniques, and officer safety.
e. Firearms safety, handling, and qualification requirements, consistent with Section 5.6.
f. PREA standards and sexual abuse prevention, reporting, and response.

g. Professional conduct, ethics, and standards of behavior under this PWS.
h. First Aid/CPR/AED and Bloodborne Pathogens awareness (OSHA -compliant).
i. Infectious disease prevention and biohazard response, including current CDC and ICE guidance.
j. Vehicle operations, safe driving practices, and emergency vehicle procedures.
k. Radio procedures, communications protocols, and use of GPS and dispatch systems.
l. ICE Form G391 procedures and any other applicable chain- of- -custody and documentation requirements.
m. Emergency response and contingency operations (e.g., vehicle accidents, medical emergencies, disturbances).
n. Confidentiality, privacy, and handling of PII and other sensitive information.

8.1.3 The contractor shall tailor initial training content by position (e.g., transport officers, dispatchers, supervisors) to ensure that each role receives the specific knowledge and skills required for successful performance.

8.2 ANNUAL REFRESHER TRAINING AND RE-QUALIFICATION

8.2.1 The contractor shall provide annual refresher training to all personnel performing work under this contract. Annual refresher training shall be not less than eight (8) hours in duration per year, unless otherwise approved by the Government.

8.2.2 Annual refresher training shall, at a minimum:

a. Reinforce key policies and procedures, including use of force, PREA, emergency response, and detainee handling.
b. Address any policy changes, lessons learned, or recurring deficiencies identified through quality assurance reviews, incident reports, or Government feedback.
c. Include updates on infectious disease protocols, safety requirements, and any new ICE or DHS directives affecting contract performance.

8.2.3 All armed personnel shall complete firearms re-qualification at least annually, using a course of fire approved by ICE and administered by a state or nationally- certified- firearms instructor.

8.2.4 The contractor shall ensure that any personnel whose firearms qualification or other critical certification has lapsed are immediately removed from duties requiring that qualification until it is restored.

8.3 SPECIALIZED AND ADVANCED TRAINING

8.3.1 The contractor shall promptly provide additional training when new policies, procedures, systems, or equipment are introduced that materially affect how personnel perform their duties.

8.3.2 The contractor shall coordinate with the COR to ensure that any specialized training is aligned with ICE standards and operational needs.

8.4 TRAINING DOCUMENTATION AND RECORDS

8.4.1 The contractor shall establish and maintain an individual training file for each employee assigned to this contract. At a minimum, each file shall include:

a. Records of all initial training completed, including dates, topics, hours, and instructor names.
b. Records of all annual refresher training, specialized training, and any remedial training completed.
c. Documentation of firearms qualification and re-qualification, including course, score, and date.
d. Certificates or proof of completion for First Aid/CPR/AED, PREA training, and any other required certifications.
e. Records of required DHS/ICE trainings (e.g., Cybersecurity Awareness, Privacy, Unauthorized Disclosure).

8.4.2 Training records shall be maintained electronically in a manner that allows near real time access and retrieval by the contractor and, upon request, by the Government.

8.4.3 The contractor shall ensure that training records are retained for the duration of the contract and for any additional period required by applicable record retention policies or contract clauses.

8.4.4 The contractor shall submit a Monthly Personnel and Training Status Report to the COR no later than the fifth (5th) calendar day of each month. At a minimum, the report shall include:

a. A complete roster of all personnel assigned to the contract (including name, position, duty location/county, and hire date).
b. Current status of background/suitability, licenses, and certifications for each individual.
c. Training completed during the reporting period, by employee and topic.
d. Upcoming expirations (within ninety (90) days) for licenses, certifications, and critical training.
e. Any training deficiencies and planned corrective actions.

8.4.5 The contractor shall ensure all mandatory DHS/ICE trainings (e.g., Cybersecurity Awareness, Privacy, Unauthorized Disclosure) are completed at the required frequency and are reflected in the training records and monthly reports.

9.0 FACILITY, EQUIPMENT, AND SUPPLIES

9.0.1 The contractor shall furnish, operate, and maintain all facilities, vehicles, equipment, and supplies necessary to perform the requirements of this PWS, except where explicitly provided as Government furnished- property or space.

9.0.2 All contractor furnished facilities, vehicles, equipment, and supplies shall meet applicable federal, state, and local laws and regulations, as well as all applicable DHS/ICE standards and policies.

9.1 DISPATCH CENTER – ICE 287(g) NATIONAL COORDINATION CENTER

9.1.1 The Government will make space available within the ICE 287(g) National Coordination Center in the greater Nashville, Tennessee area for the contractor's 24/7 dispatch operations.

9.1.2 The contractor shall be responsible, at its own expense, for equipping, furnishing, and maintaining the assigned dispatch space and for ensuring it is adequate to support continuous operations (24/7/365).

9.1.3 The contractor shall not establish alternate or backup dispatch locations without prior written approval from the COR and the CO. Any approved alternate or backup dispatch locations shall meet the same security, technical, and operational standards as the primary dispatch center.

9.1.4 The dispatch center shall provide, at a minimum, the following technical capabilities:

a. Creating and hosting a secure website which contains and displays operational data.

b. Reliable voice and data communications with all field teams and relevant ICE points of contact.
c. GPS tracking of every transport vehicle.
d. Computer aided- dispatch (CAD) or equivalent system capable of logging all requests, assignments, and status changes.
e. Capability to electronically generate, transmit, receive, and archive ICE Form G-391 and related documentation.
f. Call recording and storage for all incoming and outgoing dispatch communications, retained in accordance with contract and legal requirements.
g. While it is not anticipated that the contractor will need access to DHS/ICE information systems, the contractor shall ensure that its own systems and networks used to support dispatch operations implement appropriate security controls for safeguarding ICE data and comply with all applicable contract security and privacy requirements.

9.2 CONTRACTOR ADMINISTRATIVE AND STAGING FACILITIES

9.2.1 The contractor shall provide, at no cost to the Government, any administrative offices, armories, vehicle staging areas, training facilities, and maintenance facilities required to support operations in the State of Texas.

9.2.2 Administrative and staging facilities shall be located and managed in a manner that supports the response time- requirements and geographic coverage standards outlined in Section 5.0.

9.2.3 All armories and weapons storage locations shall meet applicable federal, state, and local requirements, as well as ICE and DHS standards, for physical security and access control.

9.2.4 The contractor shall ensure that all facilities used to support this contract are clean, safe, and maintained in a condition appropriate for law enforcement- support operations.

9.3 VEHICLES (CONTRACTOR FURNISHED)

9.3.1 The contractor shall provide, at its own expense, all vehicles necessary to meet the performance requirements of this contract.

9.3.2 All transport vehicles shall, at a minimum:

a. Be current model (or recent- model) vans or large SUVs.
b. Provide secure seating capacity for at least four (4) detainees.
c. Be equipped with a full steel security partition separating detainees from staff.
d. Be equipped with appropriate safety restraints for detainees and staff in accordance with applicable law and policy.
e. Include secure weapon storage/lockers that are not accessible to detainees.
f. Include panic/duress capability (e.g., emergency signaling or alert system) that can notify dispatch or emergency services.

9.3.3 Vehicles shall comply with Federal Motor Carrier Safety Regulations (49 CFR Parts 390–399), applicable state motor vehicle requirements, and any ICE transportation standards referenced in this PWS.

9.3.4 The contractor shall ensure that all vehicles are maintained in a safe and roadworthy condition at all times and that required inspections, registrations, and insurance are current.

9.4 PORTABLE FIELD EQUIPMENT

9.4.1 The contractor shall issue to every transport team, at a minimum, the following operational equipment:

a. Ruggedized portable thermal printer capable of printing Forms G-391 and other required documents.
b. Rugged laptop or tablet with cellular connectivity capable of accessing the secure web portal and dispatch systems.
c. Encrypted two way- radios and/or secure cell phones for continuous communication with dispatch and, when necessary, ICE personnel.
d. Restraint equipment, such as steel handcuffs, leg irons, waist chains, flex cuffs, consistent with ICE standards.
e. Detainee restraint chair capability, if required by ICE policy or specific operational needs.
f. STOP-THE-BLEED or equivalent trauma kit, including tourniquets, chest seals, hemostatic gauze, and other critical items.
g. Biohazard and infectious disease kits, including nitrile gloves, N95 or equivalent masks, face shields or eye protection, disinfectant, and red biohazard waste bags.
h. Flashlights or other suitable portable lighting equipment, as appropriate for operating conditions.

9.4.2 All portable equipment shall be maintained in 100 percent operational condition. The contractor shall implement daily checks and document any deficiencies and corrective actions.

9.4.3 The contractor shall promptly repair or replace damaged, lost, or inoperable equipment to ensure no degradation in mission capability.

9.5 EQUIPMENT ACCOUNTABILITY AND REPORTING

9.5.1 The contractor shall establish and maintain an inventory and accountability system for all vehicles, weapons, communications devices, protective gear, and other equipment used to support performance under this contract.

9.5.2 The inventory system shall be capable of identifying, at a minimum, the item, serial number (if applicable), assigned location or individual, status (in service/out of service), and any loss or damage history.

9.5.3 The contractor shall conduct periodic (at least quarterly) physical inventories of critical equipment (e.g., firearms, radios, laptops/tablets, etc) and shall reconcile any discrepancies. Losses, thefts, or unexplained discrepancies shall be reported to the COR and, where appropriate, to law enforcement, in accordance with- Section 6.7.

9.5.4 The contractor shall submit a Quarterly Equipment Inventory and Armory Reconciliation Report to the COR no later than the fifteenth (15th) calendar day after the end of each fiscal quarter, or as otherwise directed by the COR. At a minimum, the report shall include:

a. Current inventory of firearms, ammunition, by type and count.
b. Summary of any equipment loss, damage, or discrepancy identified during the reporting

period and associated corrective actions.
c. Status of critical equipment (e.g., radios, laptops/tablets, trauma kits) by location or team.

9.5.5 The contractor shall retain equipment and inventory records for the duration of the contract and any additional period required by applicable record retention requirements.

10.0 HEALTH, SAFETY, AND EMERGENCY STANDARDS

10.0.1 The contractor shall establish, implement, and maintain comprehensive health, safety, and emergency protocols that fully comply with ICE National Detention Standards (NDS) 2026, PREA standards, ICE Use of Force Policy, ICE transportation standards, CDC guidelines, and all applicable federal, state, and local laws and regulations.

10.0.2 The contractor shall ensure that all personnel understand and adhere to these health, safety, and emergency protocols at all times during performance under this contract.

10.1 DISTURBANCE PREVENTION AND USE OF FORCE

10.1.1 The contractor shall emphasize prevention, deescalation, and professional communication to minimize disturbances, confrontations, and use- of- force- incidents during transport and related activities.

10.1.2 Transport teams shall employ verbal de-escalation as the primary response to disruptive or non-compliant behavior, consistent with their training and ICE Use of Force Policy.

10.1.3 Use of force by contractor personnel shall:

a. Be limited to the minimum level of force that is objectively reasonable and necessary to restore order, prevent escape, or protect the safety of detainees, contractor personnel, ICE personnel, or the public.
b. Be consistent with ICE Use of Force Policy and applicable law.
c. Immediately cease once the threat or resistance has been controlled.

10.1.4 Any use of force beyond routine, non-resistant application of restraints shall be reported and documented in accordance with ICE policy and this PWS.

10.1.5 For each reportable use-of-force incident, the contractor shall:

a. Document the incident on form G-391, including a description of the event, force used, injuries (if any), and personnel involved; and
b. Prepare a separate Use of Force Incident Report detailing the circumstances, sequence of events, actions taken, and any medical attention provided.

10.1.6 The Use of- Force Incident Report shall be submitted via the secure portal within two (2) hours of the incident, unless otherwise directed by the COR.

10.1.7 The contractor shall cooperate fully with any ICE or other law enforcement investigation or review of a use-of-force incident and shall implement corrective actions as directed by the Government.

10.2 SEXUAL ABUSE/ASSAULT PREVENTION AND PREA COMPLIANCE

10.2.1 The contractor shall maintain a strict zero tolerance- policy for sexual abuse, sexual assault, and sexual harassment of detainees.

10.2.2 All personnel shall receive initial and annual PREA training, consistent with Section 8.0, which shall cover:

a. Definitions and examples of prohibited conduct;
b. Duty to report;
c. Procedures for reporting allegations or suspicions; and
d. Protection of detainees from retaliation for reporting.

10.2.3 Each employee shall sign an acknowledgment of PREA training and the contractor's zero tolerance policy, and these acknowledgments shall be maintained- in the employee's training file.

10.2.4 The contractor shall immediately report any allegation, suspicion, or knowledge of sexual abuse or assault involving detainees to:

a. The COR;
b. ICE Joint Intake Center (1-877-2-INTAKE or other designated reporting mechanism);
c. DHS Office of Inspector General, as required; and
d. ICE Office of Professional Responsibility (OPR), as applicable.

10.2.5 Upon receipt of an allegation or indication of sexual abuse or assault involving contractor personnel, the contractor shall immediately:

a. Remove the accused employee from any contact with detainees; and
b. Bar the accused employee from further performance under this contract pending the outcome of the investigation and any Government direction.

10.2.6 The contractor shall preserve all relevant evidence, documentation, and electronic records related to alleged sexual abuse/assault incidents and shall cooperate fully with all investigative authorities.

10.2.7 Deliverable: Annual PREA training completion roster and signed training acknowledgments, submitted in accordance with the Monthly Personnel and Training Status Report requirements in Section 8.4.

10.3 INJURY, ILLNESS, AND MEDICAL EMERGENCIES

10.3.1 The contractor shall ensure that every transport officer maintains current First Aid/CPR/AED certification through the American Red Cross or an equivalent nationally recognized organization.

10.3.2 In the event of a medical emergency involving a detainee, contractor employee, or member of the public during transport or related activities, the transport team shall:

a. Immediately notify dispatch of the situation, including nature of the emergency and location;
b. Request Emergency Medical Services (EMS) as appropriate;
c. Render appropriate first aid and/or life-saving measures within the scope of their training; and
d. Divert to the nearest appropriate medical facility when necessary, consistent with safety and guidance from dispatch and ICE.

10.3.3 Transport teams shall not accept custody of individuals who are obviously injured, unconscious, or in need of immediate medical attention unless and until the individual has been evaluated and cleared by medical personnel, and such clearance is appropriately documented.

10.3.4 All medical incidents and emergencies involving detainees shall be documented on Form G-391 and in a separate Medical Emergency Report that includes:

a. Description of the incident and symptoms observed;
b. Actions taken by contractor personnel;
c. Time EMS was requested and arrived (if applicable);
d. Medical facility to which the individual was transported (if applicable); and
e. Any known outcome or diagnosis, if available from medical personnel.

10.3.5 The Medical Emergency Report shall be submitted via the secure portal within two (2) hours of the incident or as otherwise directed by the COR.

10.3.6 The contractor shall cooperate fully with any Government review or investigation of serious injuries, illnesses, or deaths occurring during transport.

10.4 INFECTIOUS DISEASE PREVENTION AND CONTROL

10.4.1 The contractor shall comply with current CDC, ICE, and Texas Department of State Health Services guidance related to COVID-19 and other communicable diseases, as well as any additional directives issued by ICE during the period of performance.

10.4.2 The contractor shall implement written protocols for:

a. Screening for signs or symptoms of infectious illness prior to and during transport, as directed by ICE;
b. Use of appropriate personal protective equipment (PPE) by personnel and detainees when indicated;
c. Isolation or separation procedures for detainees with suspected communicable disease, as directed by ICE; and
d. Post-exposure response and reporting for personnel who may have been exposed to infectious disease.

10.4.3 Every transport vehicle shall be equipped with:

a. N95 or equivalent respirators;
b. Nitrile gloves;
c. Face shields or appropriate eye protection;
d. Hand sanitizer meeting CDC standards; and
e. EPA approved- surface disinfectant effective against relevant pathogens.

10.4.4 Vehicles shall be cleaned and disinfected after every transport, in accordance with Section 5.5 and current infectious disease guidance.

10.4.5 The contractor shall maintain documentation of sanitation procedures for each vehicle and shall make such records available to the COR upon request.

10.4.6 Deliverable: Monthly Infectious Disease Prevention Compliance information, incorporated in or submitted with the Monthly Fleet Readiness and Sanitation Report required under Section 5.5.

11.0 EMERGENCY PREPAREDNESS AND CONTINUITY OF OPERATIONS

11.0.1 The contractor shall develop, maintain, and implement a comprehensive Emergency Preparedness and Contingency Plan (EPCP) that ensures uninterrupted 287(g) transportation services during natural disasters, man-made incidents, mass arrests, civil unrest, or other large-scale disruptions that may affect operations.

11.0.2 The EPCP shall address both short-term incidents (e.g., localized outages, severe weather) and -long-term- disruptions (e.g., extended facility closures, large-scale disasters) and shall be fully integrated with ICE ERO and 287(g) partner coordination processes.

11.1 EMERGENCY PREPAREDNESS AND CONTINGENCY PLAN (EPCP)

11.1.1 The contractor shall submit an initial EPCP to the COR for review and approval no later than forty-five (45) calendar days after contract award.

11.1.2 The contractor shall review and update the EPCP at least annually. Updated versions shall be submitted to the COR for approval no later than the anniversary date of the initial plan.

11.1.3 The contractor shall also update and resubmit the EPCP within ten (10) calendar days following any major incident, full scale- exercise, or significant policy or operational change that materially affects emergency preparedness or continuity arrangements.

11.1.4 The EPCP shall, at a minimum, include:

a. An organizational chart for emergency operations, including roles, responsibilities, and 24/7 contact information for key contractor personnel.
b. A communication plan, including primary and redundant communication systems (e.g., radios, cellular, satellite phones) and escalation protocols.
c. Surge staffing procedures, including how additional teams, supervisors, and support staff will be mobilized and managed.
d. Vehicle mobilization procedures, including prioritization, staging, and reallocation of vehicles during emergencies and surges.
e. Identification of alternate staging and operating locations by region, including any pre-arranged agreements or leases.
f. Continuity of dispatch operations, including backup power, redundant connectivity, backup dispatch locations (if approved), and remote operation capability.
g. Coordination protocols with ICE ERO field offices, the National Coordination Center, 287(g) partners, and local/state emergency management agencies.
h. Hazard -specific procedures for Texas, including hurricane, flood, wildfire, and winter storm scenarios, as well as any other regionally significant threats.
i. Fuel and supply chain resiliency measures, including backup fuel sources, fuel rationing priorities, and critical supply inventories (e.g., PPE, restraints, vehicle parts).
j. Detainee safety and welfare procedures during extended or delayed operations, including provisions for food, water, climate control, and restroom access as applicable to transport duration and conditions.

11.1.5 The contractor shall ensure that all relevant personnel are familiar with the EPCP and trained on their roles and responsibilities within it.

11.1.6 The contractor shall maintain copies of the current EPCP at the dispatch center and any key administrative or staging facilities and shall make the plan available electronically to the COR upon request.

11.1.7 Deliverable: Emergency Preparedness and Contingency Plan (initial and annual updates), submitted in accordance with the schedule in Sections 11.1.1–11.1.3.

11.2 EMERGENCY OPERATIONS AND SURGE RESPONSE

11.2.1 During declared emergencies, natural disasters, or directed surge operations, the contractor shall implement the EPCP and shall prioritize life safety, security of detainees, and continuity of critical transportation services.

11.2.2 The contractor shall maintain the ability to rapidly scale operations (staffing, vehicles, and support) to meet surge requirements identified by ICE, including but not limited to:

a. Increased transport volume within specific geographic areas;
b. Simultaneous operations across multiple regions;
c. Deployment of additional teams to support mass arrest or mass processing operations.

11.2.3 The contractor shall ensure that key command and control functions (e.g., dispatch, communications, incident tracking) remain fully operational throughout emergency and surge conditions, utilizing backup systems and alternate sites as defined in the EPCP.

11.2.4 The contractor shall promptly inform the COR of any conditions that may significantly impact its ability to meet performance requirements and shall provide a mitigation plan and status updates until normal operations are restored.

11.3 REPORTING AND DOCUMENTATION

11.3.1 For any major incident affecting contractor operations under this contract (e.g., natural disaster, civil unrest, major system outage, or significant facility disruption), the contractor shall:

a. Notify the COR as soon as practicable, but no later than two (2) hours after becoming aware of the incident;
b. Provide an initial situation report (SITREP) that summarizes the nature of the incident, current and anticipated impact on operations, and any immediate mitigation measures; and
c. Provide periodic updates as requested by the COR until normal operations are restored or a new steady state- is established.

11.3.2 Within ten (10) calendar days after resolution of a major incident, the contractor shall submit a written Incident After Action-Report that includes:

a. A timeline and description of the incident and its impact on operations;
b. Actions taken by the contractor before, during, and after the incident;

c. Coordination with ICE, 287(g) partners, and other authorities;
d. Identified strengths, gaps, and lessons learned; and
e. Proposed or implemented corrective and preventive actions.

11.3.3 The contractor shall maintain records of all EPCP versions, exercises, SITREPs, and After Action Reports for the duration of the contract and any required retention period, and- shall provide them to the Government upon request.

12.0 DELIVERABLES AND REPORTING REQUIREMENTS

12.0.1 The contractor shall provide all reports and deliverables identified in this section, as well as any additional reports reasonably requested by the COR or other authorized ICE officials in support of contract oversight, performance monitoring, and mission needs.

12.0.2 All deliverables shall be prepared using ICE approved versions of Microsoft Office (e.g., Word, Excel, PowerPoint) or PDF, as specified, and shall be submitted- electronically- via the designated secure web portal or email, unless otherwise directed by the COR.

12.0.3 All deliverables shall be clear, accurate, complete, and submitted on or before the due dates specified in this section. Late, incomplete, or inaccurate deliverables may be considered in performance evaluations and may affect payment in accordance with the contract.

12.1 TRANSPORTATION MANAGEMENT OFFICE (TMO) MONTHLY REPORT

12.1.1 The contractor shall prepare and submit a monthly report to the ICE Headquarters Transportation Management Office (TMO), with a courtesy copy to the COR.

12.1.2 The TMO Monthly Report shall include, at a minimum:

a. All data elements required in the G-391 Excel Upload Template (Attachment X or successor format) for every trip completed during the reporting period; and
b. A copy of the COR Monthly Performance Report, if applicable, or other summary requested by TMO.

12.1.3 The contractor shall submit the TMO Monthly Report within five (5) business days after submission of any invoice for transportation services for that month, or as otherwise directed by TMO.

12.1.4 ICE reserves the right to update the G-391 Upload Template or to modify the means of uploading transportation data to address issues, expand capabilities, or improve performance and data quality. The contractor shall promptly implement such updates at no additional cost to the Government.

12.2 RECURRING AND EVENT -DRIVEN DELIVERABLES

12.2.1 The contractor shall provide the deliverables listed below, in addition to the TMO Monthly Report, in direct support of statewide 287(g) armed ground transportation operations.

12.2.2 Unless otherwise specified, the COR is the primary recipient for all deliverables, with copies provided to other ICE offices as directed.

12.2.3 The following table summarizes key deliverables, frequency, and format. (In Word, you may format this as a table.)

12.2.3.1 Quality Control Plan (QCP)
a. Description: A comprehensive internal Quality Control Plan documenting inspection processes, checklists, independent quality control inspectors, audit schedules, root cause- analysis procedures, corrective action tracking, and customer feedback mechanisms.
b. Frequency / Due Date:
- Initial: No later than thirty (30) calendar days after contract award.
- Updates: Annually and upon significant change in processes or scope.
c. Format / Recipient: PDF and editable Word; submitted to COR (with copy to alternate COR, if designated).

12.2.3.2 Emergency Preparedness and Contingency Plan (EPCP)
a. Description: Full EPCP with all required sections (surge operations, communications, alternate sites, mass arrest response, hazard -specific procedures, fuel resiliency, and exercise plan), as described in Section 11.0.
b. Frequency / Due Date:
- Initial: No later than forty five- (45) calendar days after contract award.
- Updates: Annually and within ten (10) calendar days after any major incident or significant policy/operational change affecting emergency preparedness.
c. Format / Recipient: PDF and editable Word; submitted to COR (with copy to alternate COR, if designated).

12.2.3.3 Weekly Phase In Status Report (Transition- In- Period Only)
a. Description: Weekly status of transition -in activities, including counties staffed, personnel in pipeline/training/background, vehicles delivered/modified, and secure portal development milestones.
b. Frequency / Due Date: Every Monday during the 120 day transition- in- period.
c. Format / Recipient: Excel and PDF; submitted to COR.

12.2.3.4 Transition Out Plan
a. Description: Detailed plan for orderly transition of services to a successor contractor or the Government, including data transfer, property return, and coordination arrangements.

b. Frequency / Due Date: No later than ninety (90) calendar days prior to contract expiration or as directed by the CO for early termination.
c. Format / Recipient: PDF and editable Word; submitted to COR and CO.

12.2.3.5 Insurance Certificates
a. Description: Current certificates of insurance meeting or exceeding contract and Section 16.0 requirements.
b. Frequency / Due Date:
- Initial: Within ten (10) calendar days after contract award.
- Updates: Annually and upon renewal or any material change.
c. Format / Recipient: PDF; submitted to COR and CO.

12.2.3.6 Daily Operational Report (Consolidated)
a. Description: Statewide daily summary including, at a minimum, total transport requests, detainees transported, average response time, list of any counties exceeding 30-minute average response time, total mileage with detainees, G-391 compliance percentage, incidents, and pickup/delivery locations.
b. Frequency / Due Date: By 0800 EST the next calendar day.
c. Format / Recipient: Submitted via secure web portal (automated generation preferred).

12.2.3.7 Weekly County Coverage Certification Report
a. Description: Roster listing every Texas county with the assigned team identifier, personnel names and badge numbers, vehicle plate number, primary and secondary contact numbers, and GPS verification timestamp.
b. Frequency / Due Date: Every Monday by 1000 EST
c. Format / Recipient: Submitted via secure web portal, with email backup to COR if directed.

12.2.3.8 Incident Reports (All Categories)
a. Description: Incident reports covering escapes, attempted escapes, use of force, PREA allegations, medical emergencies, vehicle accidents, serious injury/death, disturbances requiring law enforcement intervention, or other significant events. Each report shall include a complete chronology, witness statements (as available), links to body- worn or in- vehicle camera footage, photographs (if available), corrective actions taken, and root c-ause analysis.
b. Frequency / Due Date: Within two (2) hours of the incident occurrence or as otherwise directed by the COR for specific incident types.
c. Format / Recipient: Submitted via secure portal with immediate email notification to COR and other designated ICE contacts as required.

12.2.3.9 Monthly Performance Summary Report
a. Description: Comprehensive monthly summary including, at a minimum, statewide and county level response- time metrics (with heat map or equivalent), fleet readiness trends, training completion rates, PREA acknowledgment status, summary of incidents, customer feedback, and an executive- level- narrative summary.
b. Frequency / Due Date: No later than the fifth (5th) calendar day of the following month.
c. Format / Recipient: PDF with underlying data in Excel; submitted via secure portal.

12.2.3.10 Monthly Fleet Readiness and Sanitation Report
a. Description: Detailed fleet status, including number of vehicles operational, in maintenance, or out of service; maintenance completed during the period; post transport sanitation logs; fuel status/issues; and any significant damage- reports.
b. Frequency / Due Date: No later than the fifth (5th) calendar day of the following month.
c. Format / Recipient: Excel and PDF; submitted via secure portal.

12.2.3.11 Monthly Personnel and Training Status Report
a. Description: Roster of all personnel assigned to the contract, including name, position, county assignment, hire date, background/suitability status, and training/certification expiration dates (e.g., firearms qualification, First Aid/CPR/AED, PREA, CSAT, licenses).
b. Frequency / Due Date: No later than the fifth (5th) calendar day of the following month.
c. Format / Recipient: Excel and PDF; submitted via secure portal.

12.2.3.12 Quarterly Arming and Equipment Reconciliation Report
a. Description: Full accounting of all firearms, ammunition, and portable equipment, including any losses, damage, discrepancies, and corrective actions.
b. Frequency / Due Date: No later than the fifteenth (15th) calendar day of the following month.
c. Format / Recipient: Excel and PDF; submitted via secure portal.

12.2.3.13 Monthly Infectious Disease Prevention Compliance Report
a. Description: Summary of PPE inventory, sanitation compliance rate, relevant infectious disease incidents, and lessons learned or process improvements. This may be integrated into the Monthly Fleet Readiness and Sanitation Report if clearly identified.
b. Frequency / Due Date: No later than the fifth (5th) calendar day of the following month.
c. Format / Recipient: PDF; submitted via secure portal.

12.2.3.14 Secure Web Portal Uptime and Performance Report
a. Description: Monthly system performance summary, including uptime percentage, downtime incidents (date/time and duration), system response times, user statistics, and any security events or corrective actions.
b. Frequency / Due Date: No later than the fifth (5th) calendar day of the following month.
c. Format / Recipient: PDF; submitted via secure portal.

12.2.3.15 Privacy and Information Security Compliance Report
a. Description: Annual certification of full compliance with all privacy and information security requirements applicable to this contract, including training completion rates, summary of security/privacy incidents (or a statement that none occurred), and corrective actions taken.
b. Frequency / Due Date: Annually, submitted with the February monthly reporting package (or as otherwise directed by the COR).
c. Format / Recipient: PDF; submitted to COR with copy to ICE Privacy Office or designated POC.

12.2.3.16 Ad -Hoc Reports and Data Calls
a. Description: Any additional reports, data extracts, or analyses requested by the COR, Program Office, ICE ERO leadership, or other authorized officials (e.g., county specific- analysis,

detainee demographics summary, surge operation recap, special studies).
b. Frequency / Due Date: As specified by the COR, typically within 24–72 hours of request, depending on scope and urgency.
c. Format / Recipient: As specified in the request (e.g., Excel, PowerPoint, PDF, briefing format).

12.2.3.17 287(g) Partner Satisfaction Survey Results
a. Description: Summary of feedback collected from 287(g) partner agencies regarding response times, professionalism, communication, and overall quality of services, including any identified trends and corrective actions.
b. Frequency / Due Date: Quarterly, submitted with the March, June, September, and December monthly reporting packages.
c. Format / Recipient: PDF summary with underlying data in Excel; submitted via secure portal.

12.3 GOVERNMENT REVIEW AND CORRECTION OF DELIVERABLES

12.3.1 The Government will generally review deliverables within ten (10) calendar days of receipt, unless a different review period is specified for a particular deliverable or agreed to in writing.

12.3.2 If a deliverable is rejected or determined to be incomplete, inaccurate, or otherwise deficient by the Government, the COR will notify the contractor in writing and identify the deficiencies.

12.3.3 The contractor shall correct and resubmit any deficient deliverable within ten (10) calendar days of notification, or within another timeframe specified by the COR, at no additional cost to the Government.

12.3.4 Failure to submit required deliverables on time, or to correct deficiencies as required, may result in negative performance evaluations, payment withholds, or other contractual remedies as provided in the contract and applicable regulations.

Note: For convenience, the Government has incorporated the summary table below of required contract deliverables. This list is not exhaustive and may not include all required deliverables identified elsewhere in the PWS.

Deliverable / Service	Description	Frequency / Due Date	Format and Recipient
Quality Control Plan (QCP)	Comprehensive internal QCP documenting inspection processes, checklists, independent QC inspectors, audit schedules, root-cause analysis procedures, corrective action	Initial: No later than 30 calendar days after award Updated: Annually	PDF + editable Word to COR + alternate COR

Deliverable / Service	Description	Frequency / Due Date	Format and Recipient
	tracking, and customer feedback mechanisms	and upon significant changes	
Emergency Preparedness & Contingency Plan (EPCP)	Full EPCP with all required sections (surge, communications, alternate sites, mass arrest response, hurricane procedures, fuel resiliency, full-scale exercise plan, etc.)	Initial: No later than 45 calendar days after award Updated: Annually and within 10 days of major incident/policy change	PDF + editable Word to COR + alternate COR
Weekly Phase-In Status Report (during transition only)	Progress against Transition-In Plan – counties staffed, personnel in pipeline/training/background, vehicles delivered/modified, portal milestones	Every Monday during 120-day transition period	Excel + PDF to COR
Transition-Out Plan	Complete handover plan ensuring uninterrupted service and full cooperation with successor contractor	No later than 90 calendar days after award	PDF + editable Word to COR
Insurance Certificates	Current certificates of insurance meeting or exceeding Section 16.4 requirements	Initial: Within 10 days after award Updated: Annually and upon renewal/change	PDF to COR and Contracting Officer
Daily Operational Report (Consolidated)	Statewide summary to include total requests, detainees transported, average response time, counties >30 min (list), mileage with detainees, G-391 compliance %, incidents, pick-up and delivery locations, fleet readiness %, staffing compliance	By 0800 EST time next calendar day	Secure web portal (automated preferred)

Deliverable / Service	Description	Frequency / Due Date	Format and Recipient
Incident Reports (all categories – escape, use of force, PREA allegation, medical emergency, vehicle accident, serious injury/death, disturbance requiring LE)	Complete chronology, witness statements, photographs, corrective actions taken, root-cause analysis	Within 2 hours of incident occurrence	Secure portal + immediate email to COR
Monthly Performance Summary Report	Comprehensive report with response-time heat map by county and state-wide avg, fleet readiness trends, training completion rates, PREA acknowledgments, customer satisfaction scores, key metrics trends, notable incidents, and executive summary	No later than the 5th calendar day of following month	PDF + editable Excel via secure portal
Monthly Fleet Readiness & Sanitation Report	Detailed fleet status (vehicles operational/ready/down), maintenance completed maintenance, post-transport sanitation logs, fuel status, damage reports	No later than the 5th calendar day of following month	Excel + PDF via secure portal
Monthly Personnel & Training Status Report	Complete roster of all personnel (name, position, county assignment, hire date, background status, training/certification expiration dates, Texas Level III status)	No later than the 5th calendar day of following month	Excel + PDF via secure portal
Quarterly Arming & Equipment Reconciliation Report	Full accounting of all firearms, ammunition, portable equipment; note any losses/damage/discrepancies	No later than the 15th calendar day after the end of each fiscal quarter, or as directed by the COR	Excel + PDF via secure portal

Deliverable / Service	Description	Frequency / Due Date	Format and Recipient
Monthly Infectious Disease Prevention Compliance Report	Summary of PPE inventory, sanitation compliance rate, any disease-related incidents, lessons learned	No later than the 5th calendar day of following month	PDF via secure portal (included in Fleet Report acceptable)
Secure Web Portal Uptime & Performance Report	Monthly uptime percentage, downtime incidents, response times, user statistics, any security events	No later than the 5th calendar day of following month	PDF via secure portal
Privacy & Information Security Compliance Report	Annual certification of full compliance with all privacy and information security requirements applicable to this contract	Annually (February monthly submission)	PDF to COR + ICE Privacy Office
Ad-Hoc Reports and Data Calls	Any report or data extract requested by COR, Program Office, or ERO leadership (e.g., specific county analysis, detainee demographics, surge event recap)	As specified by COR (typically within 24–72 hours)	Format as specified (portal, Excel, PPT, etc.)
287(g) Partner Satisfaction Survey Results	Quarterly summary of feedback collected from 287(g) partners regarding response times, professionalism, and overall service	Quarterly (with March, June, Sept, Dec monthly reports)	PDF + raw data Excel via portal

All deliverables shall be prepared using ICE-approved versions of Microsoft Office. The Government will review deliverables within 10 calendar days. Rejected deliverables must be corrected and resubmitted within 10 days at no additional cost.

13.0 SECURE WEB PORTAL REQUIREMENTS

13.0.1 The contractor shall develop, host, operate, and maintain a secure web portal that serves as the contractor's primary operational platform and dashboard for all contract-related data, as

described in this PWS. The portal shall display real time or near real time operational data and shall provide authorized ICE personnel with appropriate access to view and download operational data.

The secure web portal is a stand-alone contractor-hosted system that is not directly connected to, or integrated with, any ICE or DHS network or information system. The portal will store and process CUI, including law enforcement sensitive data and PII/SPII, and shall be used solely to support performance of this contract.

13.0.2 The secure web portal shall support ICE ERO operational oversight, quality assurance, and reporting by providing authorized ICE users with timely access to transport, dispatch, fleet, staffing, and incident information.

13.0.3 The hosting environment and supporting infrastructure for the secure web portal shall provide security controls commensurate with handling law-enforcement sensitive data and PII/SPII, including, at a minimum:
a. Industry-standard technical, administrative, and physical safeguards providing protection equivalent to a moderate impact level under NIST-style security controls; and
b. Use of a reputable commercial hosting environment with independently audited security controls (e.g., SOC 2 Type II, ISO 27001 or comparable).

13.0.4 The contractor shall implement security and privacy controls for the secure web portal that are consistent with the protection of Controlled Unclassified Information (CUI) and PII/SPII, and shall comply with all contractual requirements for safeguarding such data.

13.1 FUNCTIONAL REQUIREMENTS

13.1.1 The secure web portal shall, at a minimum, provide the following capabilities:

a. **Real-time GPS tracking** of every transport vehicle.
b. **Electronic G-391 management**, including generation, electronic transmission to transport teams, digital signature capture by receiving ICE officers, and secure archiving.
c. **Transport database**, containing a complete, searchable record of every transport conducted under the contract from contract start date to present.
D. **Role-based access control**, allowing differentiated permissions (e.g., COR/CO with full administrative access, ICE ERO leadership with full administrative access, field personnel with limited or view -only access).
e. **Data query and export**, allowing authorized ICE users to filter, sort, and export data (e.g., to Excel, CSV, or PDF) for analysis, reporting, and audits.
f. **Dashboard and metrics**, presenting key performance indicators such as statewide and county/regional -level response times, fleet readiness, incident counts, and G-391 compliance.
g. **Document repository**, for storage and retrieval of required reports (e.g., Monthly Performance Summary, fleet reports, training reports, incident reports, AARs).
h. **Audit logging**, capturing user logins, role changes, data access, and updates to support oversight, investigations, and compliance reviews.

13.1.2 The portal shall support mobile responsive- access (e.g., via standard browsers on laptops, tablets, and smartphones) for authorized ICE users without requiring specialized client software, unless otherwise approved by ICE.

13.1.3 The contractor shall design and maintain the portal in a manner that is intuitive, user friendly, and consistent with Government usability requirements, to the extent practicable-.

13.2 AVAILABILITY, PERFORMANCE, AND RELIABILITY

13.2.1 The contractor shall ensure that the secure web portal achieves a minimum of 99.9 percent uptime each calendar month, excluding scheduled maintenance windows approved in advance by the COR.

13.2.2 Any scheduled maintenance that may impact portal availability shall:

a. Be minimized and, whenever possible, conducted during off peak hours;
b. Be coordinated with, and approved by, the COR in advance; and
c. Be communicated to users with reasonable prior notice, including expected start and end times.

13.2.3 The contractor shall implement appropriate redundancy, failover, backup, and disaster recovery mechanisms to maintain continuity of portal operations in the event of system failures, cyber incidents, or other disruptions.

13.2.4 The contractor shall continuously monitor system performance (including uptime, response time, and error rates) and shall promptly address performance issues.

13.2.5 The contractor shall submit a Monthly Secure Web Portal Uptime and Performance Report as described in Section 12.2, documenting uptime percentage, downtime incidents (date/time and duration), system response times, user statistics, and any security events or corrective actions.

13.3 SECURITY AND ACCESS CONTROL

13.3.1 The contractor shall implement robust access control mechanisms that ensure only authorized ICE and contractor users can access the secure web portal, and only to the extent required by their roles and responsibilities.

13.3.2 At a minimum, the contractor shall implement:

a. Unique user accounts (no shared accounts) for all users;
b. Strong authentication (e.g., multi-factor authentication), consistent with DHS/ICE policy;

c. Role-based access control (RBAC) with least- privilege- principles; and
d. Account provisioning and de-provisioning procedures that ensure timely removal of access when users no longer require it.

13.3.3 All data in transit between client devices and the secure web portal shall be encrypted using current, FIPS compliant protocols (e.g., TLS with FIPS- validated- modules).

13.3.4 All data at rest within the portal's hosting environment shall be encrypted using FIPS validated-cryptographic modules, to the extent required by DHS and FedRAMP guidance.

13.3.5 The contractor shall maintain detailed audit logs of security relevant- events, including:

a. User logons/logoffs and failed login attempts;
b. Account and role changes;
c. Data creation, modification, and deletion events for key records; and
d. Administrative actions and configuration changes.

13.3.6 Security incident detection, reporting, and response procedures for the portal shall comply with Section 6.7 of this PWS and all applicable ICE incident reporting requirements.

13.4 DATA OWNERSHIP, RETENTION, AND EXPORT

13.4.1 All data collected, processed, or stored in the secure web portal that relates to this contract (including transport records, GPS data, reports, and logs) is the property of ICE and the U.S. Government.

13.4.2 The contractor shall not use, disclose, or share portal data for any purpose other than performance of this contract, except as explicitly authorized in writing by the Government.

13.4.3 The contractor shall implement data retention and backup policies consistent with DHS/ICE requirements and any applicable records schedules identified by the Government. Retention periods for transport records, G-391 manifests, GPS data, incident reports, and other portal data will be established by ICE and communicated to the contractor. The contractor shall ensure that portal data is retained, archived, or deleted in accordance with these Government-specified requirements.

13.4.4 The portal shall support full and timely data export in commonly used formats (e.g., CSV, Excel, PDF, or other mutually agreed formats), to allow ICE to retain or migrate data as needed.

13.4.5 Upon contract completion or upon written direction from the CO, the contractor shall:

a. Provide ICE with a complete export of all portal data (including historical records, logs, and attachments) for at least the preceding twenty-four (24) months, or another period as specified by the Government;

b. Provide any necessary data dictionaries or schema documentation to allow ICE or a successor contractor to interpret and use the data; and
c. Certify deletion or sanitization of Government data from contractor systems in accordance with DHS/ICE requirements, subject to any legal or records retention- obligations.

13.5 IMPLEMENTATION AND GO-LIVE REQUIREMENTS

13.5.1 The contractor shall design, configure, and deploy the secure web portal during the transition-in period.

13.5.2 The secure web portal shall be fully operational (initial production capability) no later than ninety (90) calendar days after contract award, unless otherwise approved in writing by the CO.

13.5.3 Prior to go-live, the contractor shall:

a. Conduct testing of core functionalities (e.g., user access, GPS tracking, G-391 processing, reporting, data export);
b. Validate user roles and access control configurations;
c. Conduct security testing (e.g., vulnerability scanning) consistent with DHS/ICE guidance; and
d. Provide initial user orientation or training materials for ICE users, as directed by the COR.

13.5.4 The contractor shall document portal configuration, workflows, and standard operating procedures (SOPs) relevant to ICE use and shall provide such documentation to the COR upon request.

13.5.5 Any significant changes to portal architecture, hosting environment, or major functionality that may affect security, availability, or data integrity shall require prior written approval from the COR and, where applicable, ICE OCIO or other designated stakeholders.

14.0 TRANSITION-IN AND TRANSITION-OUT PLANS

14.0.1 The contractor shall ensure an orderly, timely, and fully coordinated transition-in at the start of the contract and transition-out at the end of the contract (or upon early termination), so that there is no interruption to mission-essential transportation services.

14.0.2 The contractor shall cooperate fully with the Government and, as directed, with any predecessor or successor contractor to ensure continuity of operations and orderly transfer of responsibilities, data, and relevant materials.

14.1 TRANSITION IN (PHASE-IN) REQUIREMENTS

14.1.1 The transition in period shall not exceed one hundred twenty (120) calendar days from contract award, unless otherwise authorized in writing by the CO.

14.1.2 The contractor shall submit a written Transition-In Plan to the COR and CO for review and approval no later than ten (10) calendar days after contract award.

14.1.3 At a minimum, the Transition-In Plan shall include:

a. Detailed schedule and milestones for achieving Full Operational Capability (FOC) within 120 days of award.
b. Recruitment, hiring, and onboarding plan, including timelines for background investigations, suitability determinations, and licensing (e.g., Texas Level III Commissioned Armed Security Officer licenses).
c. Training and qualification schedule for all personnel, including firearms, First Aid/CPR/AED, PREA, and all other required training.
d. Vehicle acquisition, modification, inspection, and deployment plan, including security outfitting, camera installation, and GPS integration.
e. Establishment of administrative, armory, and staging facilities in Texas.
f. Dispatch center setup within the ICE 287(g) National Coordination Center, including communications, IT systems, and staffing.
g. Development, testing, and deployment schedule for the secure web portal, consistent with Section 13.0.
h. Risk management and mitigation strategies for key transition in- risks (e.g., delays in hiring, licensing, vehicle outfitting, or system integration).
i. Communication protocols with the COR, ICE field offices, and 287(g) partners during the transition period.

14.1.4 **Full Operational Capability (FOC)** is defined, at a minimum, as:

a. 100 percent Texas county coverage consistent with response -time requirements in Section 5.2.
b. Dispatch operations fully functional 24/7/365 from the designated location.
c. All required vehicles and equipment in place, inspected, and mission -ready.
d. Sufficient personnel hired, vetted (EOD authorized-), trained, and qualified to meet all performance requirements.
e. Secure web portal operational with core functionalities implemented (e.g., GPS tracking, G-391 management, dashboards, and reporting).

14.1.5 The contractor shall submit a Weekly Phase In- Status Report (see Section 12.2) every Monday during the transition-in period, summarizing progress against the Transition- In Plan, including:

a. Counties activated and staffed.
b. Personnel hiring, background/suitability status, and training completion.
c. Vehicles acquired, modified, and placed into service.
d. Status of dispatch center setup and operations.

e. Status of secure web portal development, testing, and deployment.
f. Issues, risks, and mitigation actions.

14.1.6 The COR will determine and formally confirm when FOC has been achieved. The contractor shall promptly address any deficiencies identified by the COR before FOC is certified.

14.2 TRANSITION-OUT REQUIREMENTS

14.2.1 The contractor shall perform all transition-out activities in a manner that ensures uninterrupted delivery of transportation services up to and including the final day of the contract performance period.

14.2.2 The contractor shall submit a written Transition -Out Plan to the COR and CO for review and approval no later than ninety (90) calendar days prior to contract expiration, or earlier if directed due to anticipated early termination or follow on- award timing.

14.2.3 At a minimum, the Transition-Out Plan shall include:

a. Proposed schedule for transition-out activities and key milestones.
b. Approach for coordinating with the Government and any successor contractor to ensure continuity of operations.
c. Plan for transfer of operational knowledge, procedures, and points of contact.
d. Plan for data export and transfer, including all required records from the secure web portal and other systems, consistent with Sections 12.0 and 13.0.
e. Procedures for return of Government -furnished property and space.
f. Procedures for disposition or sanitization of Government data on contractor systems, in accordance with DHS/ICE requirements.
g. Staffing drawdown plan that avoids gaps in coverage and preserves required response times until contract end.
h. Risk mitigation strategies for any identified transition out- risks.

14.2.4 The contractor shall, upon written direction from the COR or CO, participate in transition planning meetings and coordination calls with ICE and any successor contractor.

14.2.5 During the transition-out period, the contractor shall:

a. Continue to meet all contract performance standards, including response-time, safety, and reporting requirements.
b. Provide reasonable access to outgoing operations for familiarization and shadowing by authorized Government and successor contractor personnel, consistent with security requirements.
c. Cooperate in scheduling and conducting any joint inventories, data reviews, or system handoffs.

14.3 DATA, RECORDS, AND PROPERTY TRANSFER

14.3.1 Within fourteen (14) calendar days after contract end, or as otherwise directed by the CO, the contractor shall:

a. Return all Government furnished property (GFP) and Government- furnished information (GFI) in its possession, in good condition (reasonable wear and tear excepted), with appropriate inventories- and supporting documentation.
b. Provide a complete inventory of contractor-furnished items used in performance, as requested by the Government (for reference and potential coordination with successor operations).
c. Provide a full export of required electronic data from the secure web portal and other systems, including, at a minimum, the previous twenty four- (24) months of transport records, logs, reports, and key documentation, along with necessary data dictionaries and schema.

14.3.2 The contractor shall ensure that all personnel and privacy sensitive records, training records, and security documentation required by the contract or by law are transferred, retained, or destroyed in accordance with DHS/ICE requirements and any applicable records schedules.

14.3.3 After verifying successful transfer of Government data and property, the contractor shall, upon written authorization from the CO or COR, sanitize or securely delete residual Government data from contractor systems in accordance with DHS/ICE security requirements and shall provide a written certification of completion.

14.4 COOPERATION WITH SUCCESSOR CONTRACTOR

14.4.1 For at least thirty (30) calendar days following contract expiration, or as otherwise directed by the CO, the contractor shall provide reasonable cooperation to the successor contractor at no additional cost to the Government. This may include:

a. Participation in coordination meetings and briefings.
b. Clarification of prior practices, procedures, and local considerations.
c. Limited, short-term overlap of operations to ensure a smooth handoff, as directed by the COR.

14.4.2 Such cooperation shall not be construed as extending the term of this contract or altering any rights of the Government regarding re-competition, follow- on- awards, or other acquisition strategies.

15.0 CONTRACTOR RESPONSIBILITIES AND QUALITY CONTROL

15.0.1 The contractor is solely responsible for the complete and timely performance of all requirements in this PWS and the resulting contract, in strict accordance with applicable laws, regulations, DHS/ICE policies, and the highest professional standards.

15.0.2 The Government will not exercise day-to-day supervision or control over contractor employees. The contractor shall provide all necessary management, supervision, and oversight to ensure that performance requirements and Acceptable Quality Levels (AQLs) are consistently met or exceeded.

15.0.3 The contractor shall ensure that all subcontractors, if any, comply with the same requirements, standards, and policies that apply to the prime contractor under this contract.

15.1 GENERAL RESPONSIBILITIES

15.1.1 The contractor shall:

a. Ensure continuous, uninterrupted performance of all mission-critical services required by this PWS, including during emergencies, surges, and periods of lapsed appropriations.
b. Maintain staffing levels, qualifications, training, and equipment sufficient to meet all response time-, safety, and reporting requirements.
c. Implement and enforce policies and procedures that support safety, security, professionalism, and compliance with ICE standards.
d. Immediately notify the COR of any condition that may materially impact the contractor's ability to meet contract requirements and provide a mitigation plan.
e. Cooperate fully with Government inspections, audits, investigations, and performance reviews.

15.1.2 The contractor shall promptly correct any identified deficiencies in performance, training, staffing, equipment, or documentation, at no additional cost to the Government.

15.2 QUALITY CONTROL PROGRAM (QCP)

15.2.1 The contractor shall establish, implement, and maintain an internal Quality Control Program (QCP) that ensures continuous monitoring and verification of compliance with every requirement in this PWS, including the performance standards and AQLs identified in Appendix A (QASP).

15.2.2 The contractor shall submit a written Quality Control Plan (QCP) to the COR for review and approval no later than thirty (30) calendar days after contract award. The approved QCP shall be incorporated into the contract and become a binding requirement.

15.2.3 The QCP shall, at a minimum:

a. Identify organizational structure and lines of authority for quality control, including quality control personnel who are functionally independent from operations.
b. Describe inspection methods and frequencies for all major performance areas (e.g., transport

operations, dispatch, vehicle readiness, documentation, training, security).
c. Include daily, weekly, and monthly quality checks (e.g., ridealongs-, file reviews, system audits) and how results are documented.
d. Provide procedures for monitoring and verifying compliance with key metrics in the QASP (e.g., response times, fleet readiness, Form G-391 compliance, portal availability).
e. Describe processes for identifying, documenting, and analyzing deficiencies, including root -cause analysis.
f. Outline corrective and preventive action procedures, including timelines, responsible parties, and follow up- verification.
g. Include a process for obtaining and analyzing customer feedback from ICE ERO personnel and 287(g) partners, and for addressing identified concerns.
h. Address how quality control information will be integrated with reporting requirements (e.g., Monthly Performance Summary Report, incident reports, fleet reports).

15.2.4 The contractor shall review and update the QCP at least annually and whenever significant changes occur in operations, policies, or risk environment. Updated QCPs shall be submitted to the COR for review and approval.

15.2.5 The contractor shall maintain records of all QC inspections, findings, and corrective actions, and shall provide such records to the COR upon request.

15.3 GOVERNMENT QUALITY ASSURANCE AND QASP

15.3.1 The Government will evaluate contractor performance using the Quality Assurance Surveillance Plan (QASP) at Appendix A, which sets forth performance standards, AQLs, and surveillance methods.

15.3.2 The Government may use any combination of the following methods to assess performance, including but not limited to:

a. Automated monitoring via the secure web portal, GPS, and system timestamps.
b. Random unannounced inspections, ride-alongs, and field observations.
c. Review of required reports and deliverables (e.g., daily, weekly, monthly, incident, and training reports).
d. Interviews and feedback from ICE staff, 287(g) partners, and other stakeholders.
e. Formal and informal performance reviews and data calls.

15.3.3 The Government's use of the QASP does not relieve the contractor of its responsibility to manage and monitor its own performance under the QCP.

15.3.4 When the Government identifies unacceptable performance or non-compliance, the COR may issue a written notice, which may include a Contract Discrepancy Report (CDR), in accordance with Appendix A.

15.3.5 The contractor shall acknowledge receipt of any CDR in writing within twenty-four (24) hours and, when requested, provide a written Corrective Action Plan (CAP) within the timeframe- specified by the COR (typically five (5) to ten (10) calendar days).

15.3.6 The CAP shall, at a minimum:

a. Describe the deficiency or non-compliance;
b. Identify root causes;
c. Specify corrective actions and implementation timelines;
d. Identify responsible individuals; and
e. Describe measures to prevent recurrence.

15.3.7 Failure to correct identified deficiencies or repeated non-compliance may result in contractual remedies, including but not limited to:

a. Payment reductions or withholds consistent with the QASP and contract terms;
b. Stop-work orders for specific activities;
c. Adverse performance ratings; or
d. Termination for default or cause, as applicable.

15.4 SUBCONTRACTING

15.4.1 The contractor shall not subcontract any portion of the work under this contract without prior written approval from the CO, with coordination by the COR.

15.4.2 Any request to use subcontractors shall include:

a. The name and address of the proposed subcontractor;
b. Description of the work to be performed by the subcontractor;
c. Subcontractor qualifications and relevant experience; and
d. Assurance that the subcontractor will comply with all applicable contract requirements (e.g., security, training, reporting).

15.4.3 The prime contractor remains fully responsible and accountable to the Government for the performance of all subcontractors and for ensuring that subcontractor performance meets all contract requirements, including QCP and QASP standards.

15.4.4 Subcontractor personnel are subject to all the same security, suitability, training, conduct, and performance requirements as contractor personnel under this PWS.

15.5 CONTINUOUS IMPROVEMENT

15.5.1 The contractor shall continuously seek opportunities to improve the efficiency, effectiveness, and safety of transportation and dispatch operations, consistent with ICE policies and the terms of this contract.

15.5.2 The contractor shall use data trends, incident analyses, customer feedback, and QC/QASP results to identify improvement opportunities and shall propose process changes or enhancements to the COR, as appropriate.

15.5.3 Any proposed changes that may affect contract requirements, performance standards, or security must receive prior written approval from the COR and, when required, the CO.

16.0 GOVERNMENT-FURNISHED PROPERTY AND INFORMATION (GFP/GFI)

16.0.1 The Government may provide certain property, space, systems access, and information to the contractor for use in performing this contract, as described in this section.

16.0.2 All Government furnished property (GFP) and Government-furnished information (GFI) shall remain the property of the U.S. Government at all times. The contractor shall use GFP and GFI solely for purposes of performing this contract and shall protect such property and information in accordance with- applicable laws, regulations, and DHS/ICE policies.

16.0.3 The contractor shall be responsible for the proper receipt, safeguarding, use, maintenance, and accountability of all GFP and GFI provided under this contract.

16.1 GOVERNMENT-FURNISHED PROPERTY (GFP)

16.1.1 The Government will provide, subject to availability and at its sole discretion, space within the ICE 287(g) National Coordination Center in the greater Nashville, Tennessee area for the contractor's centralized dispatch operations, as described in Section 9.1.

16.1.2 The Government may, at its sole discretion, provide limited access to certain ICE systems and equipment (e.g., workstations, terminals, network connections) necessary to perform dispatch and coordination functions, subject to DHS/ICE security, access control, and Rules of Behavior requirements.

16.1.3 Except as explicitly stated in this PWS or elsewhere in the contract, no other property, equipment, or facilities will be furnished by the Government.

16.1.4 The contractor shall:

a. Maintain an inventory of all GFP received, including description, serial number (if applicable), condition, and location.

b. Use GFP only for authorized purposes related to the performance of this contract.
c. Protect GFP from loss, damage, misuse, theft, or unauthorized access.
d. Promptly report any loss, damage, or theft of GFP to the COR and, when appropriate, to ICE security or law enforcement in accordance with Section 6.7 (Security Incidents and Reporting).
e. Not relocate GFP from the authorized location(s) without prior written approval from the COR.

16.1.5 At the end of the contract, or upon written direction from the CO or COR, the contractor shall return all GFP in its possession, in good condition (normal wear and tear excepted), and shall provide inventories and documentation as required under Section 14.3.

16.2 GOVERNMENT-FURNISHED INFORMATION (GFI)

16.2.1 The Government will provide, as necessary and at its discretion, GFI to enable the contractor to perform required services under this contract. GFI may include, but is not limited to:

a. Electronic copies of ICE Form G-391 and any other standard ICE forms required for detainee transport and documentation.
b. Current 287(g) partner contact lists and points of contact for state and local law enforcement agencies participating in the 287(g) Program.
c. Directories of ICE ERO field offices, sub-offices, and designated delivery locations in Texas, Oklahoma, New Mexico, and any other authorized locations.
d. Emergency contact rosters for ICE ERO, the National Coordination Center, and other relevant ICE components.
e. Applicable ICE policies, standards, and guidance documents necessary for contract performance.

16.2.2 The contractor shall treat all GFI as controlled government information and shall:

a. Use GFI solely for purposes of performing this contract.
b. Restrict access to GFI to personnel who have a valid need to know and appropriate authorization.
c. Protect GFI from unauthorized disclosure, alteration, or destruction in accordance with DHS/ICE privacy, security, and records management policies.
d. Not reproduce, distribute, or otherwise share GFI outside the contract team without prior written approval from the COR or other authorized ICE official.

16.2.3 Upon completion of the contract or upon written direction from the CO or COR, the contractor shall return or, if directed, securely destroy GFI in accordance with DHS/ICE records and information management requirements, and shall provide written certification of destruction as applicable.

16.3 SYSTEMS ACCESS AND USE OF GOVERNMENT SYSTEMS

16.3.1 If the Government provides access to ICE systems (e.g., EAGLE, ENFORCE, NCIC/TCIC query capability, or other applications) for use by contractor dispatch personnel, such access shall be governed by DHS/ICE IT security policies, Rules of Behavior, and any applicable Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA).

16.3.2 Contractor personnel granted access to Government systems shall:

a. Complete all required security and system-specific training prior to being granted access.
b. Sign and comply with all applicable Rules of Behavior and user agreements.
c. Use Government systems solely for official contract-related purposes.
d. Not attempt to bypass or disable security controls, monitoring, or logging.
e. Immediately report any suspected or actual security incidents in accordance with Section 6.7.

16.3.3 The Government reserves the right to limit, suspend, or revoke system access for any contractor employee for security, performance, or misconduct reasons, at its sole discretion. The contractor shall promptly remove affected personnel from duties requiring such access and shall provide replacements as needed.

16.4 LIABILITY FOR GOVERNMENT-FURNISHED PROPERTY

16.4.1 The contractor may be held liable for loss of or damage to GFP when such loss or damage results from negligence, willful misconduct, or failure to follow contract requirements, applicable regulations, or written directions of the Government.

16.4.2 The CO will determine liability and any appropriate remedies in accordance with the Federal Acquisition Regulation (FAR) and applicable DHS/ICE policies.

16.4.3 The contractor shall not dispose of, cannibalize, or otherwise alter GFP without express written authorization from the CO.

17.0 INVOICING AND PAYMENT

17.0.1 This contract is anticipated to be awarded on a firm fixed- price (FFP) basis, with prices established in the contract Schedule (e.g., by Contract Line Item Number (CLIN) and, as applicable, -SubCLIN-). The contractor shall perform all work described in this PWS for the fixed prices specified in the contract.

17.0.2 The contractor shall submit invoices in accordance with the terms and conditions of the contract, applicable Reimagine FAR Overhaul (RFO) and Department of Homeland Security Acquisition Regulation (HSAR) clauses, and any specific instructions issued by the Contracting Officer (CO).

17.0.3 Invoices shall be submitted electronically through the invoicing system specified in the contract (e.g., the Government's designated electronic invoicing portal) and in the format prescribed by the CO.

17.1 INVOICING REQUIREMENTS

17.1.1 The contractor shall submit invoices no more frequently than monthly, unless otherwise authorized in writing by the CO.

17.1.2 Each invoice shall, at a minimum, include:

a. Contract number and, if applicable, task or delivery order number.
b. Contractor name, address, and unique entity identifier as specified in the contract.
c. Invoice number and invoice date.
d. Invoice period of performance (e.g., "1–31 January 202X").
e. CLIN and SubCLIN- numbers, with a brief description of the services covered.
f. Firm fixed- price amounts due by CLIN/-SubCLIN (e.g., monthly- or other fixed billing unit), consistent with the contract Schedule.
g. Any approved adjustments (e.g., reductions or withholds directed by the CO) clearly identified and explained.
h. Name and contact information for the contractor representative responsible for invoice matters.

17.1.3 Invoices shall be supported by the required performance and reporting documentation for the billing period, including, at a minimum:

a. Monthly Performance Summary Report (see Section 12.2).
b. TMO Monthly Report and G-391 Excel Upload Template (see Section 12.1).
c. Monthly Fleet Readiness and Sanitation Report (if applicable to the CLIN structure).
d. Monthly Personnel and Training Status Report.
e. Monthly Arming and Equipment Reconciliation Report.
f. Any other deliverables due for that month under Section 12.0.

17.1.4 The contractor's submission of an invoice shall constitute a representation that the invoiced services have been performed in accordance with the contract requirements and that performance for the billing period meets or exceeds the applicable performance standards and Acceptable Quality Levels (AQLs) contained in Appendix A (QASP).

17.2 PAYMENT AND ACCEPTANCE

17.2.1 Payment will be made in accordance with the Prompt Payment Act, applicable FAR/HSAR clauses, and the specific terms of the contract, subject to:

a. Government acceptance of the services for the billing period; and
b. Receipt of a proper, complete, and accurate invoice.

17.2.2 The COR will review invoices and associated performance documentation and will recommend acceptance or non-acceptance to the CO. Only the CO is authorized to make binding determinations regarding invoice approval, payment, or adjustment.

17.2.3 The Government's review of invoices may include verification of:

a. Compliance with response-time, fleet readiness, and other performance requirements.
b. Timely submission and adequacy of required reports and deliverables.
c. Resolution of any known deficiencies or incidents affecting performance during the billing period.

17.2.4 The Government's failure to identify an error or omission in an invoice at the time of first review does not waive the Government's right to assert that the invoice, or a portion thereof, is improper or unallowable at a later date, consistent with applicable law and contract terms.

17.3 WITHHOLDS, ADJUSTMENTS, AND REMEDIES

17.3.1 Although this is a firm fixed-price contract, the Government reserves the right to reduce or withhold payment for a particular billing period to reflect:

a. Failure to meet one or more critical performance standards or AQLs identified in Appendix A (QASP);
b. Failure to deliver required reports or deliverables, or submission of materially deficient deliverables, not corrected within the required timeframe; or
c. Other contract non-compliance as determined by the CO.

17.3.2 Any reductions or withholds will be determined by the CO in accordance with the QASP, the terms of the contract, and applicable acquisition regulations. The CO may, for example:

a. Apply performance-based deductions or percentage reductions as specified in the contract;
b. Temporarily withhold a portion of the monthly FFP amount pending receipt of corrected deliverables or remedial performance; or
c. Apply other contractual remedies, including issuance of a Contract Discrepancy Report (CDR) and requirement for a Corrective Action Plan (CAP).

17.3.3 If performance deficiencies are subsequently corrected to the satisfaction of the Government, the CO may, at his/her discretion and consistent with the contract terms, release all or part of previously withheld amounts.

17.3.4 Payment reductions, withholds, or other remedies shall not relieve the contractor of its obligation to fully perform all requirements under this contract or to correct identified deficiencies at no additional cost to the Government.

17.4 FINAL PAYMENT AND CLOSEOUT

17.4.1 Final payment under this contract will not be made until:

a. All contractual work requirements have been completed;
b. All required deliverables, data, and reports (including final versions of required records, as applicable) have been submitted and accepted;
c. All Government furnished property and information have been returned or disposed of in accordance with- Sections 14.3 and 16.0; and
d. Any outstanding performance issues, claims, or invoice disputes have been resolved.

17.4.2 The contractor shall submit a final invoice clearly marked as “Final Invoice” in accordance with the instructions provided by the CO at the end of the contract.

17.4.3 Submission and acceptance of the final invoice shall be in accordance with applicable FAR/HSAR closeout procedures and any additional instructions provided by the CO.

APPENDIX A – QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

A.1 INTRODUCTION

A.1.1 This Quality Assurance Surveillance Plan (QASP) establishes the Government's methodology and processes for monitoring, evaluating, and documenting contractor performance under the DHS/ICE 287(g) Texas Statewide Transportation contract.

A.1.2 The purpose of this QASP is to ensure that the contractor consistently delivers safe, secure, humane, and expeditious statewide armed ground transportation services that meet or exceed the performance requirements, standards, and Acceptable Quality Levels (AQLs) set forth in the Performance Work Statement (PWS).

A.1.3 The contractor is responsible for managing its own performance and quality control under the internal Quality Control Program (QCP) required by Section 15.2 of the PWS.

A.1.4 The QASP is a government document. The Government's role in quality assurance is to:

a. Verify that contractor performance meets contractual requirements and AQLs;
b. Identify performance trends, strengths, and deficiencies;
c. Provide timely feedback to the contractor; and
d. Support the CO in making informed decisions regarding payment, remedies, and past performance.

A.2 GOVERNMENT ROLES AND RESPONSIBILITIES

A.2.1 **Contracting Officer (CO)**
The CO is responsible for all contractual actions, including:

a. Award, modification, and termination of the contract;
b. Interpretation of contract terms and conditions;
c. Determination of the adequacy of contractor performance;
d. Approval, adjustment, or disapproval of invoices; and
e. Application of contractual remedies (e.g., payment withholds, CDRs, termination).

Only the CO has authority to change the contract or commit the Government.

A.2.2 **Contracting Officer's Representative (COR)**
The COR is the primary technical representative of the CO and is responsible for:

a. Conducting day-to-day surveillance of contractor performance;
b. Reviewing and evaluating contractor deliverables and reports;
c. Documenting performance, including strengths and deficiencies;
d. Recommending corrective actions and providing technical direction within the scope of the

contract; and
e. Providing performance input to the CO, including support for invoice review and past performance evaluations.

The COR is not authorized to modify the contract or direct changes that affect price, scope, or schedule.

A.2.3 **Alternate COR(s)** (if designated)
Alternate CORs may be designated to provide backup coverage for the COR and may perform some or all COR functions as delegated in writing by the CO.

A.2.4 **Other Government Personnel**
Other ICE personnel (e.g., field staff, 287(g) partner liaisons, technical specialists) may support quality assurance by:

a. Providing feedback on contractor performance;
b. Participating in inspections, ride-alongs, or data reviews; and
c. Supporting COR/CO in investigations and performance assessments.

A.3 PERFORMANCE STANDARDS AND ACCEPTABLE QUALITY LEVELS (AQLs)

A.3.1 Performance standards and AQLs define the measurable expectations for contractor performance. The Government will evaluate whether the contractor meets, exceeds, or falls short of these standards.

A.3.2 The table below summarizes the key performance requirements, AQLs, and sample surveillance/impact. (Format as a table in Word.)

A.3.3. In the event that acceptable quality levels are not maintained to the extent of the contract requirements, the government may consider performance-based remedies such as invoice withholding or deductions.

Table A-1 – Key Performance Requirements and AQLs

Item	Performance Requirement	Acceptable Quality Level (AQL)	Measurement Method	Govt Action if AQL Not Met
1	Statewide average 30-min response time from dispatch notification to on-scene arrival at the pickup location (PWS 5.2)	100% Statewide average less than or equal to 30 minutes for each monthly period	Dispatch logs; GPS track data; secure web portal timestamps; daily reports; monthly performance summary	COR documents deficiency; CO may issue CDR, require CAP, and consider performance-based remedies (including payment adjustments) consistent with the contract and Section 17.0

Item	Performance Requirement	Acceptable Quality Level (AQL)	Measurement Method	Govt Action if AQL Not Met
2	Form G-391 complete, accurate, and electronically signed by receiving ICE officer within 15 minutes of delivery (PWS 5.5)	100% compliance each month	Secure portal audit; Daily/Monthly performance reports	COR documents deficiencies; CO may require CAP, direct remedial training or process changes, and consider appropriate contractual remedies if non-compliance is repeated or systemic.
3	Daily Operational Report submitted by 0800 EST next calendar day (PWS 12.2)	100% on time submission	Portal timestamp; COR review	COR documents late/missing reports; CO may require CAP and consider administrative or payment related- remedies if issues are recurring or impact oversight.
4	Fleet operational readiness (vehicles fully mission-capable and available to meet operational needs) (PWS 5.5, 9.3)	≥ 80% monthly average	Monthly Fleet Readiness & Sanitation Report; spot checks	COR documents deficiency: CO may require CAP and consider performance-based remedies under the contract, especially if readiness shortfalls affect response- time- performance or safety.
5	Zero preventable escapes or walk-aways of detainees while in contractor custody (PWS 5.1, 10.1)	0 preventable incidents	Incident reports & formal investigation; COR/OPR findings	Any preventable escape is treated as a critical event. CO may issue CDR, require immediate CAP, remove implicated personnel, and consider serious contractual remedies up to and including termination.
6	Zero substantiated PREA violations involving contractor personnel (PWS 6.4, 10.2)	0 substantiated incidents	ICE OPR / Joint Intake Center investigations; incident reports	Any substantiated PREA violation is treated as a critical event. CO may direct immediate removal of personnel, require CAP, and consider contract termination and other remedies under applicable law and policy.
7	Secure web portal availability meets contractual standard (PWS 13.2)	99.9% uptime per calendar month (excluding approved maintenance)	Automated system monitoring logs; Monthly Secure Web Portal Uptime and	COR documents downtime; CO may require CAP and consider performance based remedies or additional- technical requirements if availability standards are not consistently met.

Item	Performance Requirement	Acceptable Quality Level (AQL)	Measurement Method	Govt Action if AQL Not Met
			Performance Report	
8	Full Operational Capability (FOC) achieved by the end of the transition in period (PWS 14.1)	FOC achieved no later than Day 120 after award, as certified by COR	Weekly Phase In- Status Reports; COR validation of coverage, staffing, dispatch operations, and portal functionality	COR documents delay; CO may withhold or adjust payment, require CAP, and consider additional remedies as appropriate under the firm fixed- -price contract.

A.4 CONTRACTOR QUALITY CONTROL PLAN (QCP) INTERFACE

A.4.1 The contractor's QCP is the primary mechanism by which the contractor internally manages and assures quality. The QCP must align with this QASP and cover all critical performance areas.

A.4.2 The Government will review and approve the QCP but will not manage it. The contractor retains full responsibility for implementing effective internal controls and inspections.

A.4.3 The Government expects the QCP to include, at a minimum:

a. Defined inspection points and sampling plans for each critical task (e.g., transport operations, dispatch, documentation, vehicle maintenance, training, security).
b. Daily vehicle and equipment inspections and pre/post- trip- checks.
c. Monthly internal audits of Forms G-391, incident reports, and training records.
d. Random unannounced ridealongs- and field checks.
e. Root cause- analysis and corrective action tracking for all identified deficiencies.
f. Mechanisms for capturing and acting on feedback from ICE ERO and 287(g) partners.

A.5 GOVERNMENT SURVEILLANCE METHODS

A.5.1 The Government will use a risk-based mix of surveillance methods to monitor performance, including but not limited to the following:

1. **Automated Monitoring (Primary)**
    - Continuous monitoring of GPS data, timestamps, portal data, and system metrics for response times, fleet readiness, documentation compliance, and portal uptime.
    - Frequency: Continuous/ongoing.
    - Responsible: COR and designated technical staff.
2. **Document and Report Review**
    - Routine review of Daily Operational Reports, Weekly County Coverage Reports, Monthly Performance Summaries, fleet and training reports, incident reports, and EPCP/QCP updates.
    - Frequency: Daily, weekly, monthly, quarterly, and annually, as applicable.
    - Responsible: COR and alternate COR(s).
3. **Random Ride-Alongs and Field Inspections**
    - Unannounced ride-alongs, site visits to staging locations, and spot checks of vehicles, equipment, and personnel compliance with uniform and conduct standards.
    - Frequency: As determined by COR (e.g., up to a specified number per month).
    - Responsible: COR, alternate COR(s), and designated ICE field personnel.
4. **Dispatch Center Inspections**
    - On-site inspections of dispatch operations, staffing, call handling, system performance, and documentation.
    - Frequency: At least monthly, or as directed by the COR.
    - Responsible: COR/technical staff.
5. **Customer Feedback and Partner Surveys**
    - Collection and review of feedback from ICE ERO personnel and 287(g) partner agencies, including formal satisfaction surveys and informal feedback.
    - Frequency: Quarterly and ongoing.
    - Responsible: COR, with possible support from ICE HQ or field offices.
6. **Ad-Hoc Data Calls and Special Studies**
    - Targeted analyses or data calls related to specific issues (e.g., patterns in incidents, performance variations by region, surge operation reviews).
    - Frequency: As required by COR/CO.
    - Responsible: COR/CO with contractor support.

A.6 PERFORMANCE RATINGS

A.6.1 The Government may assign performance ratings monthly, quarterly, and annually, and will also provide input for formal past performance systems (e.g., CPARS) as required.

A.6.2 Performance may be assessed at the overall contract level and, as appropriate, by major task area (e.g., transport operations, dispatch, documentation, fleet readiness).

A.6.3 Ratings may follow a scale similar to the following (or as specified by DHS/ICE policy):

- **Exceptional:** Performance significantly exceeds contractual requirements. Contractor demonstrates outstanding quality, reliability, and initiative, with no significant deficiencies.
- **Very Good:** Performance exceeds many contractual requirements and is of high quality, with only minor issues quickly resolved.
- **Satisfactory:** Performance meets contractual requirements. Any deficiencies are minor, infrequent, and promptly corrected.
- **Marginal:** Performance does not fully meet some contractual requirements. Deficiencies occur and require Government oversight or direction to correct.
- **Unsatisfactory:** Performance fails to meet one or more critical requirements or AQLs. Serious or persistent deficiencies impact mission or safety; significant corrective action is required.

A.7 DOCUMENTING PERFORMANCE AND HANDLING DEFICIENCIES

A.7.1 The COR will maintain a complete quality assurance file that includes surveillance records, inspection reports, incident summaries, correspondence, and relevant performance data.

A.7.2 When unacceptable performance or non-compliance is identified, the COR will:

a. Document the issue (e.g., in surveillance logs, email, or inspection reports); and
b. Notify the contractor, verbally for minor issues and in writing for significant or recurring issues.

A.7.3 For significant or recurring deficiencies, the COR may recommend that the CO issue a **Contract Discrepancy Report (CDR)** to the contractor's Program Manager.

A.7.4 The CDR will typically include:

a. A description of the deficiency or non-compliance;
b. Reference to the specific PWS/QASP requirement(s);
c. Impact on mission, safety, or security (if applicable); and
d. A requirement for a written **Corrective Action Plan (CAP)** with a specified due date.

A.7.5 The contractor shall:

a. Acknowledge receipt of the CDR in writing within twenty four- (24) hours; and
b. Provide a CAP within the timeframe specified by the CO/COR (typically five (5) to ten (10) calendar days).

A.7.6 The Government will review the CAP and either approve it, request clarification, or reject it and require revisions.

A.7.7 The Government may verify CAP implementation through follow up- surveillance, inspections, or data review. Repeated or unresolved deficiencies may result in more serious contractual remedies, up to and including termination for default.

A.8 CONTINUOUS IMPROVEMENT

A.8.1 The Government encourages the contractor to identify and implement improvements that enhance safety, efficiency, and effectiveness, consistent with contract terms and ICE policy.

A.8.2 The contractor may propose process improvements, technology enhancements, or changes to procedures that support better performance outcomes, subject to prior written approval by the CO (and COR for technical concurrence).

A.8.3 The QASP is a living document and may be updated by the Government as needed to reflect changes in mission needs, risk environment, or contractual requirements. Any significant changes will be communicated to the contractor and, as appropriate, discussed in joint performance review meetings.

A.8 CONCLUSION

This Quality Assurance Surveillance Plan (QASP) describes the methods and standards the Government will use to monitor contractor performance under the 287(g) statewide transportation contract. It is intended to support consistent delivery of safe, secure, humane, and expeditious transportation services in accordance with the PWS and the terms of the contract.

The QASP is a living document and may be updated by the Government, as necessary, to address changes in mission requirements, risk, or contractual direction. Any such updates will be communicated to the contractor by the CO or COR.

Appendix B: ICE ERO Texas Sub-Offices (Current as of December 2025, however the list is subject to change at any time. These are intended as the primary delivery destinations, however deliveries may also be to federal partner facilities.)

Type	AOR	Name	Full Address
Field Office	DAL	Dallas	8101 N. Stemmons Freeway, Dallas, TX, 75247
Sub-Field Office	DAL	Amarillo	8375 East Amarillo Blvd, Amarillo, TX, 79107
Sub-Field Office	DAL	Lubbock	1205 Texas Ave, Suite 114, Lubbock, TX, 79401
Sub-Field Office	DAL	San Angelo	3197 Executive Drive, San Angelo, TX, 76904
Sub-Field Office	DAL	Anson	400 E. 2nd Street , Anson, TX, 79501
Sub-Field Office	DAL	Oklahoma City	1220 Sovereign Row, Oklahoma City, OK, 73108
Sub-Field Office	DAL	Alvarado	1209 Sunflower Ln, Alvarado, TX, 76009
Sub-Field Office	DAL	Tulsa	1603 S 101 E Avenue, Tulsa, OK, 74128
Sub-Field Office	DAL	Athens	109 W. Corsicana St. Suite 100, Athens , TX, 75751
Field Office	ELP	El Paso	11541 Montana Avenue, Ste E, El Paso, TX, 79936
Sub-Field Office	ELP	Las Cruces	1140 Commerce Drive Ste. B, Las Cruces, NM, 88011
Sub-Field Office	ELP	Albuquerque	5441 Watson Drive SE, Albuquerque, NM, 87106
Sub-Field Office	ELP	Big Spring	1901 W. 16th Street, Big Spring, TX, 79720
Sub-Field Office	ELP	El Paso	8915 Montana Ave, El Paso, TX, 79925
Sub-Field Office	ELP	Chaparral	26 McGregor Range Road, Chaparral, NM, 88081
Sub-Field Office	ELP	Roswell	500 N. Richardson Avenue, Roswell, NM, 88201
Sub-Field Office	ELP	Pecos	250 E Palmer Road, Pecos, TX, 79772
Sub-Field Office	ELP	Midland	1515 Idlewild Dr, Midland, TX, 79703
Field Office	HLG	Harlingen	1717 Zoy Street, Harlingen, TX, 78552
Sub-Field Office	HLG	Laredo	500 E. Mann Road, Suite A3, Laredo, TX, 78041
Sub-Field Office	HLG	Laredo	216 West Village Blvd, Suite 205, Laredo, TX, 78041
Sub-Field Office Annex	HLG	Corpus Christi	9149 TX-44, Corpus Christi, TX, 78406

Sub-Field Office	HLG	Los Fresnos	27991 Buena Vista Blvd, Los Fresnos, TX, 78566
Sub-Field Office	HLG	Edinberg	2202 Cornerstone Blvd, Edinberg, TX, 78539
Field Office	HOU	Houston	126 Northpoint Drive, Houston, TX, 77060
Sub-Field Office	HOU	Waco	800 Franklin Ave, Suite 153, Waco, TX, 76701
Sub-Field Office	HOU	Huntsville	7405 C1 Highway 75 South, Huntsville, TX, 77340
Sub-Field Office	HOU	Conroe	806 Hilbig Road, Conroe, TX, 77301
Sub-Field Office Annex	HOU	Conroe	500 Hilbig Road, Conroe, TX, 77301
Sub-Field Office	HOU	Houston	5520 Greens Road, Houston, TX, 77032
Field Office	SNA	San Antonio	1777 NE Loop 410, Suite 1500, San Antonio, TX, 78217
Sub-Field Office	SNA	Del Rio	866 Texas Spur 239 Suite 6, Del Rio, TX, 78840
Sub-Field Office	SNA	South Texas ICE Processing Center	566 Veteran's Drive, Pearsall, TX, 78061
Resident Office	SNA	San Antonio	3523 Crosspoint, San Antonio, TX, 78217
Sub-Field Office	SNA	Karnes County IPC	409 FM 1144, Karnes City, TX, 78118
Resident Office	SNA	Austin	300 E. 8th Street, Austin, TX, 78701
Sub-Field Office	SNA	T. Don Hutto Detention Center	1001 Welch St, Taylor, TX, 76574

APPENDIX C – CYBERSECURITY REQUIREMENTS

A.2 In accordance with ITAR 4.5.3.1 – Compliance with DHS Security Policy Terms and Conditions.

The following requirement should be incorporated into all acquisition documents for CUI REQUESTS:

Compliance with DHS Security Policy Terms and Conditions:

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Program 4300A version 13.4 Dec. 6, 2024 and attachments.

A.3 In accordance with ITAR 4.5.3.4 and ITAR 4.5.4.4 – Security Review

The following clause should be incorporated into ALL acquisition documents:

Security Review Terms and Conditions

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford ICE, including the organization of ICE Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact ICE Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to ICE. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of ICE data or the function of computer system operated on behalf of ICE, and to preserve evidence of computer crime.

A.4 In accordance with ITAR 4.5.3.7 – Supply Chain Risk Management

The following clause should be incorporated into ALL acquisition documents, but exclude services-only contracts:

Supply Chain Risk Management Terms and Conditions

The Contractors supplying the Government hardware and software shall provide the manufacturer's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNs number of those suppliers must also be provided.

Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.

The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.

The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

(i) How risks from the supply chain will be identified;

(ii) What processes and security measures will be adopted to manage these risks to the system or system components; and

(iii) How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Representative (COR/CO) 30 days post award.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents a risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standard certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the CO. Contractors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market, "previously used) components only with formal Government approval. Such components shall be procured from their original source and have them shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e., until the “end of life"). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

The Contractor is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

A.5 In accordance with White House Digital Government BYODTK – Privacy Expectations

The following passage should be included in ALL acquisition documents:

Privacy Expectations

Government contractor employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at any time, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed -through that device.

A.6 In accordance with White House Digital Government BYODTK – Mobile Information Technology Device Policy

The following passage should be included in ALL acquisition documents for Mobile devices:

Mobile Information Technology Device Usage

Users who conduct official DHS ICE business on a mobile IT device must:

a) Sign the Remote Access and Mobile IT Device User Agreement Form.

b) Operate the device in compliance with this policy, all applicable federal requirements, and the DHS ICE Remote Access and Mobile Information Technology Guide.

c) Not process or access Classified information on the device.

d) Use only approved and authorized DHS ICE owned devices to physically attach to DHS ICE IT systems.

e) Store only the minimum amount, if any, of Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) necessary to do one's work, and immediately delete the PII or ePHI when no longer needed. Users shall receive written approval from their supervisor before accessing, processing, transmitting, or storing DHS ICE Sensitive Information such as PII or ePHI.

f) Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.

g) Immediately contact the DHS ICE Service Desk and their immediate supervisor if the IT device is lost, stolen, damaged, destroyed, compromised, or non-functional.

h) Abide by all federal and local laws for using the device while operating a motor vehicle (e.g. users are banned from text messaging while driving federally owned vehicles, and text messaging to conduct DHS ICE business while driving non-government vehicles).

Users who are issued a DHS ICE owned mobile IT device must also:

a. Comply with DHS DHS Policy Directive 4300A Attachment Q.

b. Not disable or alter security features on the device.

c. Only use the DHS ICE owned device for official government use and limited personal use.

d. Reimburse the OCIO for any personal charges incurred that are above the established fixed cost for the Agency's use of the device (e.g. roaming charges incurred for personal calls).

e. Be required to reimburse DHS ICE if the mobile IT device is lost, stolen, damaged or destroyed as a result of negligence, improper use, or willful action on the employee's part and if determined by ICE.

A.7 In accordance with HSAR Class Deviation 15-01, REV 1, SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023) and determine if Alternate is required – ALTERNATE 1 (JULY 2023) use for ATO requirement.

*For Commercial Products or Services using FAR 12 – Insert clause 3052.212.70 Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (JULY 2023)

*Alternate I of 3052.204-72 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023) used for the Authority to Operate (ATO) requirement

The following clause should be incorporated in the PWS/SOW for High Risk Contracts, defined as contracts that consist of contractors or sub-contractors viewing ICE sensitive data, contracts that are performed off-site, and/or contracts that are performed out of the continental United States:

3052.204-72 SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)

(a) Definitions. As used in this clause—

Adequate Security means security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information. This includes ensuring that information hosted on behalf of an agency and information systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability protections through the application of cost-effective security controls.

Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an agency to handle, using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an

authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);

(B) Date of birth (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;

(F) Criminal history;

(G) Medical information; and

(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

Handling means any use of controlled unclassified information, including but not limited to marking, safeguarding, transporting, disseminating, re-using, storing, capturing, and disposing of the information.

Incident means an occurrence that—

(1) Actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or

(2) Constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

Information Security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

(1) Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

(2) Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

(3) Availability, which means ensuring timely and reliable access to and use of information.

Information System means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

(b) Handling of Controlled Unclassified Information.

(1) Contractors and subcontractors must provide adequate security to protect CUI from unauthorized access and disclosure. Adequate security includes compliance with DHS policies and procedures in effect at the time of contract award. These policies and procedures are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(2) The Contractor shall not use or redistribute any CUI handled, collected, processed, stored, or transmitted by the Contractor except as specified in the contract.

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

(4) Any government data provided, developed, or obtained under the contract, or otherwise under the control of the Contractor, shall not become part of the bankruptcy estate in the event a Contractor and/or subcontractor enters bankruptcy proceedings.

(c) Incident Reporting Requirements.

(1) Contractors and subcontractors shall report all known or suspected incidents to the Component Security Operations Center (SOC) in accordance with Attachment F, Incident Response, to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems. If the Component SOC is not available, the Contractor shall report to the DHS Enterprise SOC. Contact information for the DHS Enterprise SOC is accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. Subcontractors are required to notify the prime Contractor that it has reported a known or suspected incident to the Department. Lower tier subcontractors are required to likewise notify their higher tier subcontractor, until the prime contractor is reached. The Contractor shall also notify the Contracting Officer and COR using the contact information identified in the contract. If the report is made by phone, or the email address for the Contracting Officer or COR is not immediately available, the Contractor shall contact the Contracting Officer and COR immediately after reporting to the Component or DHS Enterprise SOC.

(2) All known or suspected incidents involving PII or SPII shall be reported within 1 hour of discovery. All other incidents shall be reported within 8 hours of discovery.

(3) CUI transmitted via email shall be protected by encryption or transmitted within secure communications systems. CUI shall be transmitted using a FIPS 140-2/140-3 Security Requirements for Cryptographic Modules validated cryptographic module identified on https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules. When this is impractical or unavailable, for Federal information systems only, CUI may be transmitted over regular email channels. When using regular email channels, Contractors and subcontractors shall not include any CUI in the subject or body of any email. The CUI shall be

included as a password-protected attachment with the password provided under separate cover, including as a separate email. Recipients of CUI information will comply with any email restrictions imposed by the originator.

(4) An incident shall not, by itself, be interpreted as evidence that the Contractor or Subcontractor has failed to provide adequate information security safeguards for CUI or has otherwise failed to meet the requirements of the contract.

(5) If an incident involves PII or SPII, in addition to the incident reporting guidelines in Attachment F, Incident Response, to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems, Contractors shall also provide as many of the following data elements that are available at the time the incident is reported, with any remaining data elements provided within 24 hours of submission of the initial incident report:

(i) Unique Entity Identifier (UEI);

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

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

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

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

(vi) Contract clearance level;

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

(viii) Government programs, platforms, or systems involved;

(ix) Location(s) of incident;

(x) Date and time the incident was discovered;

(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;

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

(xiii) Any additional information relevant to the incident.

(d) Incident Response Requirements.

(1) All determinations by the Department related to incidents, including response activities, will be made in writing by the Contracting Officer.

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

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

(i) Inspections;

(ii) Investigations;

(iii) Forensic reviews;

(iv) Data analyses and processing; and

(v) Revocation of the Authority to Operate (ATO), if applicable.

(4) The Contractor shall immediately preserve and protect images of known affected information systems and all available monitoring/packet capture data. The monitoring/packet capture data shall be retained for at least 180 days from submission of the incident report to allow DHS to request the media or decline interest.

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

(e) Certificate of Sanitization of Government and Government-Activity-Related Files and Information. Upon the conclusion of the contract by expiration, termination, cancellation, or as otherwise indicated in the contract, the Contractor shall return all CUI to DHS and/or destroy it physically and/or logically as identified in the contract unless the contract states that return and/or destruction of CUI is not required. Destruction shall conform to the guidelines for media sanitization contained in NIST SP 800–88, Guidelines for Media Sanitization. The Contractor shall certify and confirm the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, Guidelines for Media Sanitization, Appendix G.

(f) Other Reporting Requirements. Incident reporting required by this clause in no way rescinds the Contractor's responsibility for other incident reporting pertaining to its unclassified information systems under other clauses that may apply to its contract(s), or as a result of other applicable statutory or regulatory requirements, or other U.S. Government requirements.

(g) Subcontracts. The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees

will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(End of clause)

ALTERNATE I (JULY 2023)

When Federal information systems, which include Contractor information systems operated on behalf of the agency, are used to collect, process, store, or transmit CUI, add the following paragraphs:

(h) Authority to Operate. The Contractor shall not collect, process, store, or transmit CUI within a Federal information system until an ATO has been granted by the Component or Headquarters CIO, or designee. Once the ATO has been granted by the Government, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. Unless otherwise specified in the ATO letter, the ATO is valid for 3 years. An ATO is granted at the sole discretion of the Government and can be revoked at any time. Contractor receipt of an ATO does not create any contractual right of access or entitlement. The Government's grant of an ATO does not alleviate the Contractor's responsibility to ensure the information system controls are implemented and operating effectively.

(1) Complete the Security Authorization process. The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A Information Technology System Security Program, Sensitive Systems (Version 13.4, December 6, 2024), or any successor publication; and the Security Authorization Process Guide, including templates. These policies and templates are accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors.

(i) Security Authorization Package. The SA package shall be developed using the government-provided Security Requirements Traceability Matrix and SA templates. The SA package consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). The Contractor shall submit a signed copy of the SA package, validated by an independent third party, to the COR for review and approval by the Component or Headquarters CIO, or designee, at least 30 days prior to the date of operation of the information system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of modified documents.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the information system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in NIST SP 800–53, Security and Privacy Controls for Information Systems and Organizations, or successor publication, accessible at https://csrc.nist.gov/publications/sp. The Contractor shall address all deficiencies before submitting the SA package to the COR for review.

(2) Renewal of ATO. Unless otherwise specified in the ATO letter, the Contractor shall renew the ATO every 3 years. The Contractor is required to update its SA package as part of the ATO renewal process for review and verification of security controls. Review and verification of security controls is independent of the system production date and may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place. The updated SA package shall be submitted for review and approval by the Component or Headquarters CIO, or designee, at least 90 days before the ATO expiration date. The Contractor shall update its SA package by one of the following methods:

(i) Updating the SA package in the DHS Information Assurance Compliance System; or

(ii) Submitting the updated SA package directly to the COR.

(3) Security Review. The Government may elect to conduct periodic reviews to ensure that the security requirements contained in the contract are being implemented and enforced. The Government, at its sole discretion, may obtain assistance from other Federal agencies and/or third-party firms to aid in security review activities. The Contractor shall afford DHS, the Office of the Inspector General, other government organizations, and Contractors working in support of the Government access to the Contractor's facilities, installations, operations, documentation, databases, networks, systems, and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Component or Headquarters CIO, or designee, to coordinate and participate in review and inspection activity by government organizations external to DHS. Access shall be provided, to the extent necessary as determined by the Government (including providing all requested images), for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) Federal Reporting and Continuous Monitoring Requirements. Contractors operating information systems on behalf of the Government shall comply with Federal reporting and information system continuous monitoring requirements. Reporting requirements are determined by the Government and are defined in the Fiscal Year 2023 DHS Information Security Performance Plan, or successor publication, accessible at https://www.dhs.gov/dhs-security-and-training-requirements-contractors. The plan is updated on an annual basis. Annual, quarterly, and monthly data collection will be coordinated by the Government. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for information systems. The Contractor shall provide the COR with requested information within 3 business days of receipt of the request. Unless otherwise specified in the contract, monthly continuous monitoring data shall be stored at the Contractor's location for a period not less than 1 year from the date the data are created. The Government may elect to perform information system continuous monitoring and IT security scanning of information systems from government tools and infrastructure.

(End of clause)

3052.204-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents.

As prescribed in (HSAR) 48 CFR 3004.470-4(c), insert the following clause:

3052.204-73 NOTIFICATION AND CREDIT MONITORING REQUIREMENTS FOR PERSONALLY IDENTIFIABLE INFORMATION INCIDENTS (JULY 2023)

(a) Definitions. Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, the DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(1) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(2) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(i) Truncated SSN (such as last 4 digits);

(ii) Date of birth (month, day, and year);

(iii) Citizenship or immigration status;

(iv) Ethnic or religious affiliation;

(v) Sexual orientation;

(vi) Criminal history;

(vii) Medical information; and

(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(3) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) PII and SPII Notification Requirements.

(1) No later than 5 business days after being directed by the Contracting Officer, or as otherwise required by applicable law, the Contractor shall notify any individual whose PII or SPII was either under the control of the Contractor or resided in an information system under control of the Contractor at the time the incident occurred. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by, the Contracting Officer. The Contractor shall not proceed with notification unless directed in writing by the Contracting Officer.

(2) All determinations by the Department related to notifications to affected individuals and/or Federal agencies and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer.

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:

(i) A brief description of the incident;

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

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

(iv) Steps individuals may take to protect themselves;

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

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

(c) Credit Monitoring Requirements. The Contracting Officer may direct the Contractor to:

(1) Provide notification to affected individuals as described in paragraph (b).

(2) Provide credit monitoring services to individuals whose PII or SPII was under the control of the Contractor or resided in the information system at the time of the incident for a period beginning the date of the incident and extending not less than 18 months from the date the

individual is notified. Credit monitoring services shall be provided from a company with which the Contractor has no affiliation. At a minimum, credit monitoring services shall include:

(i) Triple credit bureau monitoring;

(ii) Daily customer service;

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

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

(3) Establish a dedicated call center. Call center services shall include:

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

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

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

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

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

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

(End of clause).

3052.204-71 Contractor Employee Access (JULY 2023), and determine if Alternate is required:

- Alternate I (July 2023)

- Alternate II (July 2023)

As prescribed in (HSAR) 48 CFR 3004.470-4(a), insert the following clause with appropriate alternates:

CONTRACTOR EMPLOYEE ACCESS (JULY 2023)

(a) Controlled Unclassified Information (CUI) is any information the Government creates or possesses, or an entity creates or possesses for or on behalf of the Government (other than classified information) that a law, regulation, or Governmentwide policy requires or permits an

agency to handle using safeguarding or dissemination controls. This definition includes the following CUI categories and subcategories of information:

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27, "Chemical Facility Anti-Terrorism Standards," and as further described in supplementary guidance issued by an authorized official of the Department of Homeland Security (including the Revised Procedural Manual "Safeguarding Information Designated as Chemical-Terrorism Vulnerability Information" dated September 2008);

(2) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (title XXII, subtitle B of the Homeland Security Act of 2002 as amended through Pub. L. 116–283), PCII's implementing regulations (6 CFR part 29), the PCII Program Procedures Manual, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security, the PCII Program Manager, or a PCII Program Manager Designee;

(3) Sensitive Security Information (SSI) as defined in 49 CFR part 1520, "Protection of Sensitive Security Information," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or designee), including Department of Homeland Security MD 11056.1, "Sensitive Security Information (SSI)" and, within the Transportation Security Administration, TSA MD 2810.1, "SSI Program";

(4) Homeland Security Agreement Information means information the Department of Homeland Security receives pursuant to an agreement with State, local, Tribal, territorial, or private sector partners that is required to be protected by that agreement. The Department receives this information in furtherance of the missions of the Department, including, but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Sharing Act of 2015;

(5) Homeland Security Enforcement Information means unclassified information of a sensitive nature lawfully created, possessed, or transmitted by the Department of Homeland Security in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department;

(6) International Agreement Information means information the Department of Homeland Security receives that is required to be protected by an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization;

(7) Information Systems Vulnerability Information (ISVI) means:

(i) Department of Homeland Security information technology (IT) systems data revealing infrastructure used for servers, desktops, and networks; applications name, version, and release; switching, router, and gateway information; interconnections and access methods; and mission or

business use/need. Examples of ISVI are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526 will be classified as appropriate; and/or

(ii) Information regarding developing or current technology, the release of which could hinder the objectives of the Department, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system;

(8) Operations Security Information means Department of Homeland Security information that could be collected, analyzed, and exploited by a foreign adversary to identify intentions, capabilities, operations, and vulnerabilities that threaten operational security for the missions of the Department;

(9) Personnel Security Information means information that could result in physical risk to Department of Homeland Security personnel or other individuals whom the Department is responsible for protecting;

(10) Physical Security Information means reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of Federal buildings, grounds, or property. For example, threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation;

(11) Privacy Information includes both Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII). PII refers to information that can be used to distinguish or trace an individual's identity, either alone, or when combined with other information that is linked or linkable to a specific individual; and SPII is a subset of PII that if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. To determine whether information is PII, DHS will perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available, in any medium or from any source, that would make it possible to identify an individual. Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration Numbers (A-numbers), financial account numbers, and biometric identifiers.

(ii) Multiple pieces of information may present an increased risk of harm to the individual when combined, posing an increased risk of harm to the individual. SPII may also consist of any grouping of information that contains an individual's name or other unique identifier plus one or more of the following elements:

(A) Truncated SSN (such as last 4 digits);

(B) Date of birth (month, day, and year);

(C) Citizenship or immigration status;

(D) Ethnic or religious affiliation;

(E) Sexual orientation;

(F) Criminal history;

(G) Medical information; and

(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

(iii) Other PII that may present an increased risk of harm to the individual depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. The context includes the purpose for which the PII was collected, maintained, and used. This assessment is critical because the same information in different contexts can reveal additional information about the impacted individual.

(b) Information Resources means information and related resources, such as personnel, equipment, funds, and information technology.

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

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

(e) Work under this contract may involve access to CUI. The Contractor shall access and use CUI only for the purpose of furnishing advice or assistance directly to the Government in support of the Government's activities, and shall not disclose, orally or in writing, CUI for any other purpose to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized to access CUI, the Contractor shall ensure that these persons receive initial and refresher training concerning the protection and disclosure of CUI. Initial

training shall be completed within 60 days of contract award and refresher training shall be completed every 2 years thereafter.

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

(End of clause)

ALTERNATE I (JULY 2023)

When the contract will require Contractor employees to have access to information resources, add the following paragraphs:

(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.

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

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).

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

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

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

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

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

(End of clause)

Alternate II (JULY 2023)

When the Department has determined contract employee access to controlled unclassified information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to information resources, add the following paragraphs:

(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

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

(End of clause)

*For Commercial Products or Services using FAR 12 – please add the following:

3052.212-70 Contract terms and conditions applicable to DHS acquisition of commercial items.

As prescribed in (HSAR) 48 CFR 3012.301, insert the following clause:

Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (JULY 2023)

The Contractor agrees to comply with any provision or clause that is incorporated herein by reference to implement agency policy applicable to acquisition of commercial items or components. The provision or clause in effect based on the applicable regulation cited on the date the solicitation is issued applies unless otherwise stated herein. The following provisions and clauses are incorporated by reference: [The Contracting Officer should either check the provisions and clauses that apply or delete the provisions and clauses that do not apply from the list. The Contracting Officer may add the date of the provision or clause if desired for clarity.]

(a) Provisions.

____3052.216-70 Evaluation of Offers Subject to An Economic Price Adjustment Clause.

____3052.219-72 Evaluation of Prime Contractor Participation in the DHS Mentor Protégé Program.

____3052.247-70 F.o.B. Origin Information.

____Alternate I

____Alternate II

____3052.247-71 F.o.B. Origin Only.

____3052.247-72 F.o.B. Destination Only.

(b) Clauses.

____3052.203-70 Instructions for Contractor Disclosure of Violations.

____3052.204–71 Contractor Employee Access.

____Alternate I

____Alternate II

____3052.204–72 Safeguarding of Controlled Unclassified Information.

____Alternate I

____3052.204–73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents."

____3052.205-70 Advertisement, Publicizing Awards, and Releases.

____Alternate I

____3052.209-72 Organizational Conflicts of Interest.

____3052.209-73 Limitation on Future Contracting.

____3052.215-70 Key Personnel or Facilities.

____3052.216-71 Determination of Award Fee.

____3052.216-72 Performance Evaluation Plan.

____3052.216-73 Distribution of Award Fee.

____3052.217-91 Performance. (USCG)

____3052.217-92 Inspection and Manner of Doing Work. (USCG)

____3052.217.93 Subcontracts. (USCG)

____3052.217.94 Lay Days. (USCG)

____3052.217-95 Liability and Insurance. (USCG)

____3052.217-96 Title. (USCG)

____3052.217.97 Discharge of Liens. (USCG)

____3052.217-98 Delays. (USCG)

____3052.217-99 Department of Labor Safety and Health Regulations for Ship Repair. (USCG)

____3052.217-100 Guarantee. (USCG)

____3052.219-71 DHS Mentor Protégé Program.

____3052.228-70 Insurance.

____3052.228-90 Notification of Miller Act Payment Bond Protection. (USCG)

____3052.228-91 Loss of or Damage to Leased Aircraft. (USCG)

____3052.228.92 Fair Market Value of Aircraft. (USCG)

____3052.228-93 Risk and Indemnities. (USCG)

____3052.236-70 Special Provisions for Work at Operating Airports.

____3052.242-72 Contracting Officer's Representative.

(End of clause)

A.8 DHS Use of Artificial Intelligence (AI) Tools

The following requirement should be incorporated into all acquisition documents for CUI REQUESTS:

(a) Compliance with Federal AI Laws and Policies; AI Use Limitations. The Contractor shall ensure that any AI system or service provided complies with all applicable federal, DHS, and ICE AI Policies, Directives, and Memos. The AI solution must align with the U.S. Constitution

and all relevant laws and regulations; including privacy, civil rights, and civil liberties. Specifically:

(1) The Contractor must stay current and comply with any updates or new AI policy requirements issued during the contract term.

(2) AI used to support law enforcement decisions or civil actions must include technical and operational safeguards to.

i. Establish human-in-the loop oversight.

ii. Document or label AI-generated content.

(3) For AI used in determinations impacting individuals (e.g., risk assessments, identity verification), the Contractor must cooperate with federal, DHS, and ICE procedures for notice and appeal, providing explanations or adjusting outputs upon error findings.

(4) The contract prohibits use of AI that violates DHS policy, including.

i. Using AI outputs as sole evidence for punitive or enforcement actions.

ii. Utilize AI to make or support decisions on improper bases (e.g. predicting future behavior or emotional state leading to discriminatory or unlawful actions).

(5) The Contractor must follow AI Use Case approval and Security Authorization processes before developing, piloting, testing, or deploying AI in ICE environments or using ICE data.

(6) The Contractor is responsible for complying with AI Security Control Baseline requirements.

(b) Transparency, Auditability and Explainability. The Contractor shall design, build, document, and operate the AI system or service to be explainable, auditable, and transparent. At a minimum, the Contractor shall:

(1) Document the provenance of data used for AI training, fine-tuning, or operation.

(2) Ensure data used for AI training, fine-tuning, or operation was lawfully obtained and processed.

(3) Document the provenance of any third-party AI models used (source, version, etc.).

(4) Provide comprehensive system diagrams and inventories that map the AI systems' API and system connections, data flows, and technical components.

(5) Provide comprehensive documentation explaining how the AI system works, including any models and algorithms.

(6) Ensure the AI system, where applicable, provides clear explanations or reasoning for its decisions or predictions.

(7) Ensure AI outputs are traceable; auditable; meet evidentiary standards; and are explainable to non-technical users. Additionally, ensure GenAI inputs and their outputs are logged and preserved in line with federal, DHS, and ICE retention policies.

(c) Data Rights and Solution Ownership. The contract shall clearly delineate data and intellectual property rights to protect ICE's interests in the AI solution and associated data. Specifically:

(1) All data provided by the Government or generated through the AI system belongs to the Government. The contractor is prohibited from:

i. Using nonpublic agency data and outputted results to train publicly or commercially available AI algorithms, or any non-ICE systems outside the contract's scope without ICE's authorization.

ii. Using Government-furnished data or AI-generated data for purposes outside the contract without ICE authorization.

iii. Sharing, disclosing, or transferring Government data, AI models, or AI-outputs with third parties without ICE's authorization.

(2) The Contractor must grant the Government appropriate license rights in any custom-developed AI models, software, or deliverables. IP rights will be negotiated consistent with federal law and the agency's mission needs, aiming to avoid vendor lock-in. The Government may require broad or unlimited rights to certain deliverables (including source code or trained model files) for long-term use, maintenance, or integration of the AI solution.

(3) ICE maintains ownership over and the Contactor must provide ICE access to:

i. Any derivative outputs of AI developed under the Contract, including data processed using AI.

ii. Any models trained, fine-tuned, or otherwise developed using ICE data.

(d) Prevention Against Vendor Lock-In. To promote a competitive marketplace and long-term sustainability of ICE's AI capabilities, the Contractor shall:

(1) Utilize industry-standards, APIs, and protocols wherever possible to ensure interoperability and combatibility within and between ICE and DHS systems.

(2) Ensure inputs and outputs of the AI system are exportable in a non-proprietary, machine-readable format to facilitate integration or transfer of functions to other systems.

(3) Where custom components are developed, deliver sufficient technical documentation and access to components (including source code, model weights, or other foundational code) to enable ICE's long-term use of the AI system.

(4) In the case of transitioning the AI system to another Contractor or in-house provider, the Contractor must support knowledge transfer and provide all necessary documentation, models, data, and software to enable sustained system use.

i. The Contract must also document estimated costs and related steps that will be required to exit the Contract.

(e) Security, Testing & Evaluation, and Continuous Monitoring: The Contractor shall implement rigorous security and risk management measures for the AI solution, per federal standards, ICE procedures, and OMB guidance on AI risks. Key requirements include:

(1) If designated as a High Impact AI system, complying with all required AI Risk Management practices (per OMB, DHS, and ICE policy), unless officially granted a waiver.

(2) Before deploying the AI system: The Contractor must provide testing and evaluation artifacts and support (including providing requisite access to enable) ICE independent test and evaluation processes to evaluate factors such as, but not limited to:

i. AI system performance, including accuracy and reliability.

ii. Compliance with DHS AI Security Controls.

iii. Resiliency against AI cybersecurity and operational threats, including system misuse/abuse.

iv. Completion of an AI impact assessment and/or other risk assessment procedures, in line with federal, DHS, and ICE policy and practices.

v. Fulfillment of functional, business, and technical requirements.

(3) While operating the AI system: The Contractor must re-test system performance, security, and resiliency before deploying new models; against misuse/abuse before deploying new AI models; fine-tuned models; or changes to AI systems that require Change Requests.

(4) Audit and Logging: Ensure compliance with DHS and ICE AI auditing and logging requirements, including, but not limited to audit and logging the access, usage, and modification of:

i. AI Guardrails deployed in GenAI systems.

ii. Models, including parameters and weights.

iii. AI system inputs and outputs (including prompts).

(f) Continuous Monitoring: The Contractor shall implement continuous monitoring mechanisms to detect and respond to anomalies, biases, or performance degradation in AI systems. Additionally:

i. The Contractor shall establish protocols for the timely remediation of identified issues, including the potential suspension of AI system operations if necessary.

ii. The Contractor shall comply with all continuous monitoring requirements, per federal, DHS, and ICE policy.

A.9 DHS FAR Class Deviation 17-03 – Revision 1

52.224-3 Privacy Training – Alternate I (DEVIATION)

(a) Definition. As used in this clause, personally identifiable information means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (See Office of Management and Budget (OMB) Circular A–130, Managing Federal Information as a Strategic Resource).

(b) The Contractor shall ensure that initial privacy training, and annual privacy training thereafter, is completed by contractor employees who—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information on behalf of an agency; or

(3) Design, develop, maintain, or operate a system of records (see also FAR subpart 24.1 and 39.105).

(c) The contracting agency will provide initial privacy training, and annual privacy training thereafter, to Contractor employees for the duration of this contract. Contractor employees shall satisfy this requirement by completing Privacy at DHS: Protecting Personal Information accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within 30 days of contract award and be completed on an annual basis thereafter not later than October 31st of each year.

(d) The Contractor shall maintain and, upon request, provide documentation of completion of privacy training to the Contracting Officer.

(e) The Contractor shall not allow any employee access to a system of records, or permit any employee to create, collect, use, process, store, maintain, disseminate, disclose, dispose or otherwise handle personally identifiable information, or to design, develop, maintain, or operate a system of records unless the employee has completed privacy training, as required by this clause.

(f) The substance of this clause, including this paragraph (f), shall be included in all subcontracts under this contract, when subcontractor employees will—

(1) Have access to a system of records;

(2) Create, collect, use, process, store, maintain, disseminate, disclose, dispose, or otherwise handle personally identifiable information; or

(3) Design, develop, maintain, or operate a system of records.

B.1 In accordance with ITAR 4.5.3.2 – Encryption Compliance

The following requirement should be incorporated into all acquisition documents for CUI REQUESTS:

Encryption Compliance Terms and Conditions

If encryption is required, the following methods are acceptable for encrypting sensitive information:

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

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

c) Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

B.2 In accordance with ITAR 4.5.3.5 and ITAR 4.5.4.5 – Interconnection Security Agreement (ISA)

If the service requested requires a connection to a non-DHS/ICE, Contractor systems, or DHS/ICE system of different sensitivity, the following requirement should be incorporated into ALL acquisition documents:

ISA Terms and Conditions

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

B.3 In accordance with ITAR 4.5.3.6 and ITAR 4.5.4.6 – Required Protections for DHS/ICE Systems Hosted in Non-DHS/ICE Data Centers

The following terms and conditions should be included for ALL information systems which are hosted, operated, maintained, and used on behalf of DHS/ICE at non-DHS/ICE facilities:

1) Security Authorization Terms and Conditions

A Security Authorization of any infrastructure directly in support of DHS/ICE information system shall be performed as a general support system (GSS) prior to DHS/ICE occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization (SA) shall be performed in accordance with DHS/ICE Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of DHS/ICE information system.

At the beginning of the contract, and upon request thereafter (generally at the deployment of a new system or renewal of a System Authority to Operate), the contractor/Cloud Service Provider (CSP) shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS/ICE applies in the SA process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into DHS/ICE POA&M Management Process. ICE shall use DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies shall be corrected within the timeframes dictated by DHS/ICE POA&M Management Process. CSP procedures shall be subject to periodic, unannounced assessments by DHS/ICE officials. The documented physical aspects associated with CSP activities shall also be subject to such assessments. Inspections of CSP physical facilities will be scheduled in advance and coordinated with the provider in accordance with their facility procedures.On a periodic basis, DHS and its Components, including DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these clauses. Evaluation could include, but is not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the CSP and reseller shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS/ICE information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS/ICE, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS/ICE in the event of a security incident.

2) Enterprise Security Architecture Terms and Conditions

The CSP shall utilize and adhere to DHS/ICE Enterprise Security Architecture in accordance with applicable laws and DHS/ICE policies to the satisfaction of DHS/ICE COR.

3) Continuous Monitoring Terms and Conditions

The CSP shall participate in the DHS/ICE Continuous Monitoring methodologies and, shall provide a Continuous Monitoring capability over their resources as required by FedRAMP. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the CSP shall adhere to all ITAR and FedRAMP continuous monitoring requirements and ensure that DHS/ICE can implement and integrate the following processes:

a) Asset Management

b) Vulnerability Management

c) Configuration Management

d) Malware Management

e) Log Integration

f) Security Information Event Management (SIEM) Integration

g) Patch Management

h) Providing near-real-time security status information to DHS/ICE SOC Specific Protections Terms and Conditions

i) Specific protections that shall be provided by the CSP include, but are not limited to the following:

Specific Operations Terms and Conditions

The Contractor shall operate a SOC to provide security for the below mentioned services. The CSP shall support regular reviews with DHS/ICE Information Security Office to coordinate and synchronize the security posture of the CSP hosting facility with that of DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The CSP staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the CSP staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the CSP facility SOC shall adhere to the incident response plan.

4) Computer Incident Response Services Terms and Conditions

The CSP shall provide Computer Incident Response Team (CIRT) services. The CSP shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS/ICE-specific incident response plan that adheres to DHS/ICE policy and procedure for reporting incidents. The CSP shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The CSP shall notify DHS/ICE SOC of any incident in

accordance with the Incident Response Plan and work with DHS/ICE throughout the incident duration.

5) Network Intrusion Detection Systems (NIDS) and Monitoring Terms and Conditions

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets for their facility(s). The NIDS solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be made available to DHS/ICE upon request. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

6) Physical and Information Security and Monitoring Terms and Conditions

The CSP shall provide a facility using appropriate protective measures to provide for physical security. All facilities will be located within the United States. The CSP shall maintain a process to control physical access to all DHS/ICE IT assets. DHS/ICE IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS/ICE security office upon request.

7) Vulnerability Assessments Terms and Conditions

The CSP and reseller shall provide all information from any managed device to DHS/ICE, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

8) Anti-malware (e.g., virus, spam) Terms and Conditions

The CSP shall design, implement, monitor, and manage to provide comprehensive anti-malware service. The CSP shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, when changes are required. A summary of alerts shall be reported to DHS/ICE SOC in weekly status report. If an abnormality or anomaly is identified, the CSP shall notify the appropriate DHS/ICE point of contact in accordance with the incident response plan.

9) Log Retention Terms and Conditions

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

B.4 In accordance with ITAR 4.5.3.8 – Personal Identification Verification (PIV) Credential Compliance

The following requirement should be incorporated into ALL acquisition documents:

Personal Identification Verification (PIV) Credential Compliance Terms and Conditions

a) Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

b) Procurements for software products or software developments shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

c) PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

d) If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

B.8 In accordance with FedRAMP

Note: The following requirements/clauses apply to both CUI and CLASSIFIED REQUESTS.

1) FedRAMP IT Systems Security Requirements

a) The Federal agency will determine the security category for the cloud system in accordance with Federal Information Processing Standard 199; then, the contractor/Cloud Service Provider (CSP) shall apply the appropriate set of impact baseline controls as required in the FedRAMP Cloud Computing Security Requirements Baseline document to ensure compliance to security standards. The FedRAMP baseline controls are based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5.1.1, Security and Privacy Controls for Federal Information Systems and Organizations (as amended), and also includes a set of additional controls for use within systems providing cloud services to the federal government.

b) The CSP shall maintain a security management continuous monitoring environment that meets or exceeds the requirements outlined in the latest edition of FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements.

2) FedRAMP Privacy Requirements

Contractor shall be responsible for the following privacy and security safeguards:

a) To the extent required to carry out the FedRAMP assessment and authorization process and FedRAMP continuous monitoring, to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the Contractor, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases.

b) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

c) The contractor shall also comply with any additional FedRAMP privacy requirements.
d) The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. In accordance with the Federal Acquisitions Regulations (FAR) clause 52.239-1, contractor shall be responsible for the following privacy and security safeguards:
(i) The Contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception—Disclosure to a Consumer Agency for purposes of C&A verification.
(ii) To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours. The program of inspection shall include, but is not limited to: Authenticated and unauthenticated operating system/network vulnerability scans Authenticated and unauthenticated we b application vulnerability scans Authenticated and unauthenticated database application vulnerability scans Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools.
(iii) If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.
(iv) If the vendor chooses to run its own automated scans or audits, results from these scans may, at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor-conducted scans shall be provided, in full, to the Government.
3) Sensitive Information Storage
Sensitive But Unclassified (CUI) information, data, and/or equipment will only be disclosed to authorize personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST SP 800-88, Guidelines for Media Sanitization.
The disposition of all data will be at the written direction of the COR, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the COR.
4) Protection of Information
The contractor shall be responsible for properly protecting all information used, gathered, or developed because of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information as sensitive. All information about the systems gathered or created under this contract should be considered as CUI information. It is anticipated that this information will be gathered, created, and stored within the primary work location. If contractor personnel must remove any information from the primary work area they should protect it to the same extent they would their proprietary data and/or company trade secrets. The

use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.
The government will retain unrestricted rights to government data. The government retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.
The data that is processed and stored by the various applications within the network infrastructure contains financial data as well as personally identifiable information (PII). This data and PII shall be protected against unauthorized access, disclosure or modification, theft, or destruction. The contractor shall ensure that the facilities that house the network infrastructure are physically secure.
The government-owned data must be available to the Government upon request within one business day or within the timeframe specified otherwise, and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.
No data shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

5) Security Classification

The preparation of the deliverables in this contract will be completed at a Sensitive but Unclassified level unless a higher level is specified.

6) Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of this contract, are the property of the U.S. Government, and must be submitted to the COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials in accordance with FAR 52.227-[applicable FAR clause number]. Federal Acquisition Regulations (FAR) clauses Numbers 52.227-1 through 52.227-23 dealing with Patent Rights, Data Rights, Royalties, etc…
All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the CO.
Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

7) Disclosure of Information

Any information made available to the Contractor by the Government shall be used only for carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any

means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

8) FedRAMP Security Requirements Overview:

a) The minimum requirements for low and moderate impact cloud systems are contained within the FedRAMP Cloud Computing Security Requirements Baseline. The contractor and Federal Government Agency share responsibility to ensure compliance with security requirements.

b) The implementation of a new Federal Government cloud system requires a formal process, known as Assessment and Authorization, which provides guidelines for performing the assessment.

c) FedRAMP requires cloud service providers to utilize a Third-Party Assessment Organization (3PAO) to perform an assessment of the cloud service provider's security controls to determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements.

d) The FedRAMP PMO security staff will be available for consultation during the process. Both the FedRAMP PMO staff and JAB will review the results before issuing a Provisional Authorization decision. The Government reserves the right to verify the infrastructure and security test results before issuing an Authorization decision.

e) Federal agencies will be able to leverage the provisional Authorization granted by FedRAMP and any documentation prepared by the contractor to issue their own authority to operate.

f) The vendor is advised to review the FedRAMP guidance documents (see References below) to determine the level of effort that will be necessary to complete the requirements. All FedRAMP documents and templates are available at http://FedRAMP.gov.

9) FedRAMP Security Compliance Requirements

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for low and moderate impact system (as defined in FIPS 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for both low and moderate impact systems. While the FedRAMP baseline controls are based on NIST SP 800-53, Revision 4. The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

10) Required FedRAMP Policies and Regulations

The contractor shall comply with FedRAMP Security Assessment Framework – describing a general security Assessment Framework for the Federal Risk and Authorization Management Program (FedRAMP). This document details the security assessment process which must be used to achieve FedRAMP compliance. Download here:
https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Assessment_Framework.pdf

11) Assessment and Authorization

DHS/ICE may choose to cancel the contract/award and terminate any outstanding orders if the contractor has its provisional authorization revoked and the deficiencies are greater than agency risk tolerance thresholds.

12) Assessment of the System

a) The contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. The contractor shall create, maintain and update the following documentation using FedRAMP requirements and templates, which are available at http://FedRAMP.gov :

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)
- IT System Contingency Plan (CP)
- IT System Contingency Plan (CP) Test Results
- POA&M Continuous Monitoring Plan (CMP)
- FedRAMP Control Tailoring Workbook
- Control Implementation Summary Table
- Results of Penetration Testing
- Software Code Review
- Interconnection Agreements/Service Level Agreements/Memorandum of Agreements.

b) Information systems must be assessed by an accredited 3PAO whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

c) The Government reserves the right to perform Penetration Testing. If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment activities to include control reviews in accordance with FedRAMP requirements (https://www.fedramp.gov/assets/resources/documents/CSP_Penetration_Test_Guidance.pdf). Review activities include but are not limited to scanning operating systems, web applications, wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

d) Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a POA&M document. Depending on the severity of the gaps, the Government may require them to be remediated before a provisional authorization is issued.

e) The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 30 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

13) Authorization of System

The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct onsite inspections.

The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

14) Reporting and Continuous Monitoring

Maintenance of the FedRAMP Provisional Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the FedRAMP PMO as required by FedRAMP Requirements. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the FedRAMP JAB to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

All deliverables shall be labeled [appropriate label such as "Controlled Unclassified Information" (CUI) or other agency-selected designation per document sensitivity]. External transmission/dissemination of [labeled deliverables] to or from a Government computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140 (as amended), "Security requirements for Cryptographic Modules."

CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide parties.

15) Non-Repudiation

The Cloud Service Provider vendor shall provide a system that is capable of implementing NIST SP 800-53 Control AU-10 approved controls, which provides for origin authentication, data integrity, and signer non-repudiation. This binds the identity of the information producer with the information to and provides the means for authorized individuals to determine the identity of the producer of the information.

16) Identification and Authentication (Organizational Users)

The vendor shall support a secure, multi-factor method of remote authentication and authorization to identified Government Administrators that will allow Government designated personnel the ability to perform management duties on the system.

The vendor shall support multi-factor authentication including [specific method of authentication]. User ID and Password, digital certificate, PIV or smart card, PIN, tokens, etc…

17) Identification and Authentication (Non-Organizational Users)

The vendor shall support a secure, dual factor method of remote authentication and authorization to identified Vendor Administrators that will allow vendor-designated personnel the ability to perform management duties on the system.

18) Incident Reporting Timeframes

Cloud Service Providers are required to report all computer security incidents to the United States Computer Emergency Readiness Team (U.S.-CERT) in accordance with U.S.-CERT "Incident Categories and Reporting Timeframes" in , Appendix J, Table J-1 of NIST SP 800-61 (as amended), "Computer Security Incident Handling Guide." Any Category (CAT) 1, CAT 2, or CAT 3 incident, must be reported immediately to their Information Systems Security Officer (ISSO) and the Senior Agency Information Security Officer (SAISO). Any incident that involves compromised Personally Identifiable Information (PII) must be reported to U.S.-CERT within 1 hour of detection regardless of the incident category reporting timeframe.

19) Media Transport

The vendor shall document activities associated with the transport of Federal agency information stored on digital and non-digital media and employ cryptographic mechanisms to protect the confidentiality and integrity of this information during transport outside of controlled areas. Digital media, containing Federal agency information, that is transported outside of controlled areas must be encrypted using a [encryption mode]; non-digital media including but not limited to CD-ROM, floppy disks, etc., must be secured using the same policies and procedures as paper. Media, containing Federal Agency information that is transported outside of controlled areas must ensure accountability. This can be accomplished through [appropriate actions such as logging and a documented chain of custody form].

Federal Agency data that resides on mobile/portable devices (e.g., USB flash drives, external hard 12 drives, and SD cards) must be encrypted using [encryption mode]. All Federal Agency data residing on laptop computing devices must be protected with approved encryption software. Encryption mode is typically Advanced Encryption Standard (AES) either 128 or 256 block size.

20) Boundary Protection

The CSP/Reseller shall route all external connections through a Trusted Internet Connection (TIC).

21) Protection of Information At Rest

The CSP shall provide security mechanisms for handling data at rest and in transit in accordance with FIPS 140-2.

22) Security Alerts, Advisories, and Directives

The CSP/Reseller shall provide a list of their personnel, identified by name and role, with system 1 administration, monitoring, and/or security responsibilities that are to receive security alerts, two advisories, and directives. This list shall include ICE SOC.

B.9 Patch Management Terms and Conditions

The following requirement should be incorporated into acquisition documents for Software-as-a-Service (SaaS) and Platform-as-a-Service (PaaS):

The CSP, or software vendor (for certain Software-as-a-Service (SaaS) offerings), shall perform patch management services to all Platform-as-a-Service (PaaS) and SaaS offerings managed by the CSP, or in cases where the SaaS offering is hosted by an independent third party, the third party will be responsible for providing the patch management services. The CSP shall push patches that are required by vendors and DHS/ICE system owner. This is to ensure that the infrastructure and applications that directly support DHS/ICE information system are current in their release and that all security patches are applied. The CSP and software vendor shall be informed by DHS/ICE which patches are required by DHS/ICE through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS/ICE utilizes to fulfill their mission, shall be tested by DHS/ICE. However, the CSP and software vendor(s) shall be responsible for deploying patches to their products as directed by DHS/ICE. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the CSP prior to deployment in a test environment.

B.10 DHS Enterprise Cloud Hosting and Non-DHS Cloud Hosting Requirements in accordance with the DHS CIO Memo – Enterprise Cloud Hosting Governance document.

The following requirement should be incorporated into all acquisition documents that are on DHS ICE Enterprise Cloud Systems or on Non-DHS ICE Cloud Hosting Systems:

1) ICE Cloud Hosting

All ICE systems and data must be hosted within the ICE Cloud environment unless a documented mission or business justification is submitted and approved in writing by the ICE Chief Information Officer (CIO). The Contractor shall not provision, operate, or maintain any separate or external cloud environment for ICE data or systems without this explicit approval.

2) Management and Telemetry for Non-ICE Cloud Hosting

If any system or data must be hosted outside the ICE Cloud, the Contractor shall ensure the system remains subject to ICE OCIO management and oversight. The Contractor must provide ICE OCIO with direct management access and ensure that all required telemetry, monitoring, and resource-level metrics are forwarded to ICE-designated tools and endpoints using ICE-approved integration methods.

3) Authorization to Operate (ATO) Requirement

No system may be made operational, nor process or store ICE data, until it has received an ICE Authorization to Operate (ATO). This requirement applies to all systems, regardless of hosting location, ownership, or management.

4) Authorization of Dependencies and Security Deliverables

Any cloud environment or system upon which an ICE system depends must be FedRAMP authorized at the appropriate impact level. If the cloud environment is not FedRAMP authorized, the Contractor must provide all necessary system security deliverables to support the ICE ATO process, regardless of ownership or management. Acceptable (but not exhaustive) examples of required artifacts include:

- System Security Plan (SSP)
- Security Assessment Report (SAR)
- Plan of Actions and Milestones (POA&M)
- Penetration test results
- Vulnerability scan results
- Continuous monitoring reports

5) Exception and Waiver Process

Any request to host ICE workloads outside of the ICE Cloud must be accompanied by a written justification, ICE CIO approval, and a transition plan. The Contractor must provide all required documentation and comply with any additional conditions imposed by ICE OCIO.

6) Coordination and Compliance

The Contractor shall coordinate with ICE OCIO, system owners, data owners, privacy, and legal leads to implement all cloud governance and security requirements. The Contractor shall promptly address any legal or operational barriers and provide regular updates to ICE OCIO.

F.1 In accordance with ITAR 4.5.3.2 – Encryption Compliance

The following requirement should be incorporated into all acquisition documents for SENSITIVE BUT UNCLASSIFIED REQUESTS:

Encryption Compliance Terms and Conditions

If encryption is required, the following methods are acceptable for encrypting sensitive information:

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

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

c) Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

F.2 In accordance with ITAR 4.5.3.8 – Personal Identification Verification (PIV) Credential Compliance

The following requirement should be incorporated into ALL acquisition documents:

Personal Identification Verification (PIV) Credential Compliance Terms and Conditions

a) Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

b) Procurements for software products or software developments shall be compliant by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

c) PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

d) If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

F.4 Patch Management Terms and Conditions

The Contractor shall perform patch management services. The Contractor shall push patches that are required by vendors and DHS system owner. This is to ensure that the infrastructure and applications that directly support DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.