SECTION C - DESCRIPTION/SPECIFICATION/WORK STATEMENT

Disclaimer: This list is illustrative only and is provided for informational purposes to convey the general scope and nature of work that may be performed under this contract. Inclusion of a project on this list does not obligate the Government to issue a task order for that project, nor does it guarantee that any task orders or awards will be made under this IDIQ contract. The Government reserves the right to issue task orders for other construction-related projects consistent with the overall scope of this contract.

C.1 General

This MACC will support primarily design-Build (DB) or performance-based construction delivery methods. Projects may include, but are not limited to new construction, renovation, demolition, repair, building system installations, and infrastructure systems. Major elements of the work may include architectural, civil, structural, mechanical, electrical, fire protection, and communication systems. Facilities may include, but are not limited to dorms, administrative buildings, medical clinics, classrooms, training centers, warehouses, roads, firing ranges. Repairs may include, but are not limited to HVAC, electrical, fire suppression, site work, and security upgrades. Renovations may involve cosmetic upgrades up to major building renovations inclusive of change of occupancy use.

C.2 Period of Performance

The overall contract will include a base period of five (5) years from the date of award. The Government may include option periods as defined in the solicitation.

Each individual Task Order issued under this contract will include its own specific period of performance and schedule, which will be defined in the Task Order documentation. Task Order durations may vary depending on the scope and complexity of the work

C.3 Performance Requirements

The contractor shall perform all work in accordance with:

- Task Order-specific technical specifications, drawings, and schedules
- Applicable codes (Industry Criteria, latest edition upon task order solicitation) including, but not limited to:

<u>American Correctional Association</u>
ACA Performance-Based Standards and Expected Practices for Adult Local Detention Facilities
(Where the ICE Detention Standards are silent, the ACA Jail Standards must be followed)

<u>American Concrete Institute</u>

ACI Manual of Concrete Practice,
ACI 315R-18, Guide to Presenting Reinforcing Steel Design Details
ACI 318-19 Building Code Requirements for Reinforced Concrete o PCA Notes on ACI 318-19
ACI 301-16 Specifications for Structural Concrete for Buildings

American Institute of Steel Construction
AISC Steel Construction Manual
AISC Seismic Design Manual
ANSI/AISC 360-22 Specification for Structural Steel Buildings
ANSI/AISC 341-22 Seismic Provisions for Structural Steel Buildings

American Iron and Steel Institute
AISI S100-16 North American Specification for the Design of Cold- Formed Steel Structural Members

American Society of Civil Engineers
ASCE 7-22 Minimum Design Loads for Buildings

American National Standards Institute
ANSI/TIA/EIA-568-B.2 Commercial Building Telecommunications Cabling Standard
ANSI/IEEE C2-2002, National Safety Electric Code.
ANSI A117.1-2017 – Accessible and Usable Buildings and Facilities
ANSI/NAAMM HMMA 863 - Guide Specifications for Detention Security Hollow Metal Doors and Frames
ANSI/AWS D1.1 - Structural Welding Code-Steel
ANSI/AWS D1.3 - Structural Welding Code - Sheet Steel

American Society of Heating, Refrigerating and Air Conditioning Engineers
ASHRAE 55 Thermal Environmental Conditions for Human Occupancy
ASHRAE 62.1 Ventilation for Acceptable Indoor Air Quality
ASHRAE 90.1 Energy Standards for Buildings Except Low-Rise Residential Buildings

American Society for Testing and Materials
ASTM A653/A653M - Specification for Steel Sheet, Zinc-Coated (Galvanized)or Zinc-Iron Alloy-Coated (Galvannealed) by the Hot-Dip Process
ASTM B117 - Standard Practice for Operating Salt Spray (Fog) Testing Apparatus
ASTM D2794 - Test Method for Resistance of Organic Coatings to the Effects of Rapid Deformation (Impact)
ASTM F33 Committee - Draft test method for steel Bunks, Seats, Tables used in detention facilities.
ASTM F2322-12- Test Methods for Physical Assaults on Fixed Barriers for Detention Facilities.
ASTM F2697-15; Physical Assault on Horizontal Fixed Barriers for Detention and Correctional Facilities.
ASTM F1450-12- Test Methods for Hollow Metal Swinging Door Assemblies for Detention Facilities

American Water Works Association Standards
AWWA C651-05

Illuminating Engineering Society
The Lighting Handbook (illumination level requirements)

International Code Council
IBC International Building Code
IMC International Mechanical Code
IPC International Plumbing Code
IECC International Energy Conservation Code
IFC International Fire Code
IFGC International Fuel Gas Code

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)
ISO/IEC 27001:2013 Information Technology-Security Techniques- Information Security Management Systems Requirements

The Masonry Society
TMS 402/602-22 Building Code Requirements and Specifications for Masonry Structures

National Design Specification
NDS-18 National Design Specification for Wood Design w/ Supplement

National Fire Protection Association (If conflicts arise in code, NFPA 101 shall be the overarching document to be followed)
NFPA 13, Installation of Sprinkler Systems
NFPA 70, National Electric Code
NFPA 70E - Electrical Workplace Safety
NFPA 72, National Fire Alarm Code
NFPA 90A Installation of Air Conditioning and Ventilating Systems
NFPA 101 Life Safety Code

- Government Criteria:

All applicable Federal, State and County Laws and requirements (including applicable State Building Codes where design requirements more stringent than IBC)

Department of Homeland Security
U.S. Immigration & Customs Enforcement Information and Communications Technology Systems Structured Cable Plant Standard, January 2025 Edition
U.S. Immigration & Customs Enforcement Service Processing Center Detention Construction Standards
U.S. Immigration & Customs Enforcement Facility Design Guide (Revised 2025) and references incorporated within the guide

U.S. Immigration & Customs Enforcement Health Services Design Standards (June 2023)
U.S. Immigration & Customs Enforcement National Detention Standards (2025)

Department of Justice
Prison Rape Elimination Act (PREA)

Federal Highway Administration
Federal Highway Administration Publication No. FHWA-NHI-01¬021, Hydraulic Engineering Circular No. 22, Second Edition, URBAN DRAINAGE DESIGN MANUAL

U.S Weather Bureau
U.S. Weather Bureau Technical Paper No. 40, dated May 1961, Rainfall Frequency Atlas of the United States for Durations from 30 minutes to 24 hours, and return periods from 1 to 100 years

United States Access Board
Architectural Barriers Act (ABA) Standards

The contractor shall:

- Ensure all work is completed in a safe, timely, and professional manner.
- Maintain a clean and secure job site at all times.
- Coordinate with Government personnel to minimize disruption to ongoing operations.
- Submit and adhere to project designs schedules, construction schedules, safety plans, and quality control plans as required by each Task Order.
- Comply with all environmental protection requirements, including proper handling and disposal of hazardous materials.
- Provide as-built drawings, warranties, training, and operation and maintenance (O&M) manuals as required by each Task Order.
- The contractor shall maintain the capability to perform multiple, concurrent task orders under this contract. This includes, but is not limited to, the ability to manage overlapping schedules, allocate resources across projects, and coordinate subcontractors and suppliers, as needed.
- The Government may issue task orders with overlapping periods of performance at different locations.
- Contractors shall demonstrate sufficient organizational, financial, and bonding capacity to support concurrent execution of task orders. Bonding capacity may be used as an indicator of the contractor's ability to manage multiple projects simultaneously.

C.4 Contractor Staff and Employees

1. Prior to the issuance of the first TO, the contractor shall provide the CO with the telephone number at which the contractor or his representative may be contacted at any time during the regular working hours and an emergency number at which the contractor may be contacted in situations requiring immediate attention. The above-mentioned representative, if provided, must have full power and authority to act upon the behalf of the contractor.

2. The contractor shall maintain a Project Manager and provide the CO a personnel list ten (10) days prior to performance of the contract. The individual designated as the project manager shall have full authority to act for the contractor. The personnel shall meet or exceed the position requirements submitted in the SOW. The Government reserves the right to approve or disapprove personnel based on the position requirements. The contractor shall provide experienced and knowledgeable personnel in civil, structural, architectural, mechanical, and electrical disciplines.

   Project Manager Qualifications: BS degree in an appropriate field in at least one of the following: (Building Engineering, Civil Engineering, Construction Management, Architecture, Construction Engineering). Shall have at least 10 years of experience managing project of similar size and value. The Project Manager must be capable of reading, writing, and conversing fluently in the English language.

3. For all Design Build contracts, the following key personnel, with applicable experience, shall be provided.

   - Designer of Record

   Designer-of-Record Qualifications: The design shall be accomplished by a professional Architecture Engineering firm (serving as the Designer of Record) with at least 5 years of experience in design related to projects of similar size, value, and scope. The Designer of Record shall be a registered professional engineer in the state of the project.

   - Registered Design Professionals

   Registered Design Professionals Qualifications: Registered Design Professionals, who will be responsible for each discipline of the design, shall be registered professionals (professional engineer, registered architect or certified by NCIDQ) in a state within the United States of America.

   - Superintendent

   Provide project superintendent with a minimum of 5 years as a superintendent on projects similar in size and complexity. The individual must be familiar with and have experience in the areas of hazard identification and safety compliance. The individual must be capable of interpreting a critical path schedule and construction drawings. The qualification requirements for the alternate superintendent are the same as for the project superintendent. Minimum Communication Requirements:

Have at least one qualified superintendent, or competent alternate, capable of reading, writing, and conversing fluently in the English language, on the jobsite always during the performance of Contract work. The project superintendent is primarily responsible for managing subcontractors and coordinating day-to-day production and schedule adherence on the project. The superintendent is required to attend partnering meetings, and quality control meetings. The superintendent or qualified alternative must be on-site at all times during the performance of this contract until the work is completed and accepted. A letter designating the superintendent shall be sent to the CO within ten (10) calendar days of receipt of the Notice to Proceed. This letter shall provide the superintendent's complete name, address, daytime and after hours phone numbers. The superintendent must have the authority to act on behalf of the contractor (FAR 52.236-6 SUPERINTENDENCE BY THE CONTRACTOR (APR 1984)). A designation letter shall be submitted for each and every task order issued under this contract.

The superintendent shall have on site the drawings and specifications for this project (FAR 52.236-21 SPECIFICATIONS AND DRAWINGS FOR CONSTRUCTION (FEB 1997)). Drawings shall be redlined (as necessary) and kept current for submission at the completion of the project. Drawings must always be available for CO's Representative (COR) review throughout the project.

- Quality Control Manager

The Quality Control Manager must be a graduate engineer, graduate architect, or a graduate of construction management, with a minimum of five years construction quality control experience on construction similar to this Contract or a construction person with a minimum of ten years of construction experience, of which a minimum of five years' experience must be in construction quality control on construction similar to this contract. The Quality Control Manager and all members of the quality control organization must be capable of reading, writing, and conversing fluently in the English language. The Quality Control Manager or qualified alternative must be on-site at all times during the performance of this contract work until the work is completed and accepted.

4. Supervision. The Government will not exercise any supervision or control over the contractor's employees performing services under this contract. Such employees shall be accountable not to the Government, but solely to the contractor, who, in turn, is responsible to the Government. At all times during the performance of each TO under this contract, and until the work under that TO is completed and accepted, the contractor shall directly oversee the work under each TO, or assign, and have on the work site, a competent representative who is satisfactory to the CO and has authority to act for the contractor. This may include a working supervisor.

5. Contractor's Employees: The contractor's employees shall adhere to the rules and regulations of the SPC applicable to employees' conduct/behavior. The CO may require, in writing, the contractor to remove from the job site any employee the CO deems incompetent, careless, or otherwise objectionable. The contractor shall select personnel

who are well qualified to perform the required work, for supervising techniques used in their work, and for keeping them informed of all improvements, changes, and methods of operation. In addition, the contractor shall take appropriate personnel action, as required, in the event employee(s) become involved with law enforcement authorities as a result of misconduct.

C.5 Management Plan

Contractor shall submit a Management Plan within 15 days of contract award. The plan shall clearly explain how the contractor's labor, resources, materials, and suppliers will be coordinated to include leveraging subcontractors to ensure successful project completion. An organizational structure depicted through a chart to articulate home office support, on site management and how the chain of command will be leveraged to address any potential issues. The organizational structure shall depict lines of authority and lines of communication. The plan should address how the offeror will address the labor challenges in this region to ensure available subcontractor skilled labor for successful project completion. The plan should address resource allocation, risk management, scheduling, and communication details.

C.6 Post-Award Conference

Before the issuance of the first task order under the contract, a post-award conference shall be conducted by the CO, with the COR in attendance, to acquaint the contractor with Government policies and procedures that shall be observed during the prosecution of the work, and to develop a mutual understanding relative to the administration of the contract. It is strongly suggested that the contractor's Project Manager, Quality Control Manager, Superintendent, and other appropriate employees attend this conference. Individual task order conference: At the discretion of the CO and/or the COR, a pre-construction conference may be conducted prior to the commencement of work on individual task orders.

C.7 Preconstruction Conference

Prior to start of construction for each individual task order, a pre-construction conference will be scheduled by the authorized representative of the Contracting Officer. The purpose of this conference is to discuss and develop a mutual understanding of the administrative requirements of the Contract including but not limited to: daily reporting, invoicing, value engineering, safety, base-access, outage requests, hot work permits, schedule requirements, quality control, schedule of prices or earned value report, shop drawings, submittals, cybersecurity, prosecution of the work, government acceptance, final inspections and contract close-out and the processes for joint risk management between the Contractor and Government. Contractor must present and discuss their basic approach to scheduling the construction work and any required phasing.

C.8 Project Schedule

Develop a project schedule for each task order. Show in the schedule the proposed sequence to perform the work and dates contemplated for starting and completing all schedule activities. The

scheduling of the entire project is required. The scheduling of design and construction is the responsibility of the Contractor. Use the Critical Path method (CPM) of network calculation to generate all project schedules. Include in the schedule activities associated with the critical submittals and their approvals, NEAPA review, procurement, fabrication, and delivery of long lead materials, equipment, fabricated assemblies, and supplies. Include in the schedule activities for submission, review, and acceptance of design packages, submission and approval of O&M Manuals, submission and approval of As-Built drawings, pe-final inspections, punch list, and final inspection.

C.9 Existing Utilities

Utility locations when shown are approximate. Provide an independent, private utility locating company to positively identify underground utilities in the work area in addition to any station locating service and coordinated with the station utility department. The third party, independent, private locating company must locate utility depth by use of Ground Penetrating Radar (GPR), X-ray, bore scope, or ultrasound prior to the start of demolition and construction. The use of historical drawings does not alleviate the Contractor from meeting this requirement. Contractor responsible to fully repair all damage caused by their activities to existing utilities.

C.10 Security Requirements

The contractor shall comply with all ICE security protocols, including but not limited to:

- Personnel background checks and badging requirements
- Escort procedures for uncleared personnel
- Protection of Government property and controlled areas
- Immediate reporting of security incidents or breaches to the Contracting Officer and Security Office

Contractors shall ensure that all personnel are trained in site-specific security procedures and that access to restricted areas is controlled at all times.

C.11 Federal Construction Management Software Usage Requirements (MACC Contract)

ICE will be using Kahua as its project management software. All project documentation and submittals will be managed through Kahua.

C.12 Compliance and Security Standards

All personnel accessing the SPC must be prior approved by the ICE Security Division. Specific

project security measures are provided elsewhere in these specifications.

The project is to be fully contained within a security fenced enclosure and access to the site is controlled via security protocols. The D-B Contractor must be responsible for constructing the perimeter security infrastructure needed to secure the site and its subsequent connection to the existing secure SPC campus and must tie into existing fiber optic perimeter fence detection system in all fencing being altered or added. Coordination with SPC personnel before removing or altering any fencing or security apparatus is required. All fencing removal and installation must be done with the plan to always provide containment at required levels.

C.13 Project Documentation and Collaboration

The Contractor shall perform all project activities including but not limited to:

- RFIs
- Submittals & Approvals
- Punch Lists
- Project Schedules
- Change Orders
- Design Reviews (for design-build)
- Progress Payments
- NEPA reviews and document preparation

C.14 Data Integrity and Audit Readiness

Contractors shall ensure:

- Complete audit trails of all transactions
- Document retention for 3 years after final payment in accordance with RFO 4.703
- Real-time budget tracking and reporting
- FOIA-compliant documentation for public transparency

C.15 Cleanup and Site Restoration

The contractor shall:

- Maintain a clean and orderly work site throughout the duration of the project
- Remove all construction debris, waste materials, and equipment upon completion of work

- Restore all disturbed areas to their original or specified condition, including landscaping, pavement, and utilities

- Dispose of all waste in accordance with federal, state, and local environmental regulations

- Conduct a final site walkthrough with the Government to verify cleanup and closeout compliance

If the Contractor fails to maintain a clean and safe work environment, the Government may decide to take corrective action or withhold payment until deficiencies are resolved.

C.16 Deliverables

The Government will define deliverables in each Task Order that may include, but are not limited to:

- Design Schedules

- Construction schedules

- Site Plan

- Design documents (35%, 65%, 95%, 100% as indicated)

- As-built drawings

- O&M Manuals

- Warranty Documentation

- Daily Progress reports

- Quality control plan and inspection reports

- Site Safety and Health plan and reports

- NEPA Categorical Exclusions, Environmental Assessments, and decisional documents (if applicable)

- LEED documentation (if applicable)

- BIM models (if applicable)

- Commissioning reports (if applicable)
- TAB reports
- Security plans (if applicable)
- Final inspection and acceptance documentation

C.17 Points of Contact

The contractor shall designate and provide the Government with primary and alternate points of contact (POCs) for task order issuance and coordination. These individuals shall be authorized by the Contractor to receive task order solicitations, respond to requests for proposals, and coordinate technical and contractual matters.

The contractor shall provide the following information for each POC:

- Full name
- Title/role
- Email address
- Direct phone number (mobile or office)

The contractor shall ensure that all POC information is kept current throughout the life of the contract. POC designations are valid until the Contracting Officer is notified of a change. Any changes to POC information shall be submitted to the Contracting Officer in writing within five (5) business days of the change.

Each IDIQ task order will designate a **Contracting Officer (CO)** and a **Contracting Officer's Representative (COR)**. All contractual matters shall be directed to the CO at the Task Order

C.18 Information Technology

1. IT Purchase Authorization

The contractor shall ensure all IT products and services direct charged to the contract are approved through the OCIO's Commercial IT Request (CITR) Application. This includes, but is not limited to, FITARA, Supply Chain Risk Management (SCRM), IPv6, and 508 compliance. No purchases of commercial IT products or services should be made prior to coordination and approval by the OCIO. Contractor shall report purchases monthly. This contract shall only be used to purchase software, software maintenance, hardware, or hardware maintenance necessary for the performance of this contract. ICE shall own the license(s) or subscriptions for any software or applications purchased. All hardware shall be titled to ICE.

2. Section 508 Conformance

The contractor shall ensure that all products, platforms, services, and communications delivered as part of this work statement, that are Information and Communication Technology (ICT) or contain ICT, conform to the Revised Section 508 of the Rehabilitation Act Standards, 36 C.F.R. § 1194.1 & Apps. A, C & D. The Standards may be found at https://www.ecfr.gov/current/title-36/section-1194.1

3. Records Management

- The Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law, including but not limited to, the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, as well as ICE records policies (NPD 1440.6, ICE Records Management Program, and NPR 1441.1, ICE Records Management Program Requirements).

- The Contractor shall ensure that ICE-owned/Contractor-held records are segregated from contractor-owned records and from non-record materials and report holdings of ICE records.

- The Contractor shall immediately notify the Contracting Officer and ICE Records Officer upon discovery of any inadvertent or unauthorized removal, defacing, alteration, or destruction of Federal records. Destruction of Federal Records is EXPRESSLY PROHIBITED unless in accordance with records retention schedules or as directed by the Contracting Officer.

- All Contractor employees assigned to this contract who create, work with, or otherwise handle Federal Records are required to complete mandatory ICE- provided records management training. The Contractor shall ensure that training has been completed according to agency policies, including initial training and any required annual or refresher training.

- The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this contract, and require written subcontractor acknowledgment of same.

4. Use of Artificial Intelligence (AI) During Contract Performance

- The contractor must disclose any potential or intended use of Artificial Intelligence (AI) technologies, tools, or systems in the performance of this contract. If it is unknown at the time of contract award whether AI will be used, the contractor must provide written notice to the Government prior to the deployment of any AI systems during contract performance. If AI technologies are introduced after the commencement of contract

performance, the contractor must notify the contracting officer in writing prior to the release or deployment of any AI component, capability, or system in the ICE environment.

- The Government reserves the right to review, approve, or disapprove the proposed use of AI technology in the performance of this contract. The contractor must obtain written approval from the contracting office before implementing AI systems.
- If any subcontractor intends to use AI technologies in the performance of work under this contract, the contractor must ensure that similar notification and disclosure requirements apply to all subcontractors. The contractor is responsible for collecting the notification and disclosure requirements from subcontractors and submitting them to the Government.

C.20 Data Requirement Deliverables (DRDs)

This section provides a description of the fields of the Data Requirement Documents (DRDs).

- DRD No.: Unique identifier for the DRD.
- DRD Title: Unique name for the DRD.
- Date: Date prepared.
- Purpose / Use: The purpose of and ICE's intended use for the DRD.
- Remarks: This field provides additional submittal information, if necessary.
- Data Requirements: This field provides the detailed description of the required and/or expected content and scope of the deliverable(s).

DATA TRANSMITTAL AND FORMAT:

This section provides additional detail regarding the transmittal and format of the DRDs.

The Contractor shall transmit Data Transmittal DRDs to ICE electronically, by hardcopy, or by other mechanism agreed to by the Contracting Officer. The Contractor shall notify the Contracting Officer and the Contracting Officer Representative (COR) in writing of DRD delivery.

Data Transmittal Package:

- For each DRD, the Contractor shall ensure the transmittal package includes:
    - Contractor transmittal memorandum that provides the following information:
        a. Contract number.
        b. Contractor name.
        c. DRD number.
        d. DRD data type (specified in "Type" column of the DRL).

e. Submission date or milestone being satisfied.
f. Document number and revision.
g. Document title.
h. File names of all files being delivered; multiple files per document must be clearly related to the document.
i. Distribution (Notification list as defined by the DRD distribution field and the Contracting Officer's letter).
j. Targeted release date.

- Electronic files submitted to the appropriate ICE or Contractor site.

---End of Section---

SECURITY 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.

POSITION DESIGNATION

IAW Title 5, CFR part 731, dated December 18, 2024, 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.

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 under 5 CFR 731 dated December 18, 2024, and DHS

Instruction 121-01-007, Revision 2, dated August 10, 2024, or successors thereto; 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)).

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), or successor thereto, in the Office of Personnel Management (OPM) 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" form completed online and archived by the contractor applicant/employee in their NBIS eAPP account.

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

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.

With respect to break-in-service requirements for transfer of trust, OPM removed the 24-month break-in-

service provision. This requirement is replaced with a new process, established in the Federal Personnel Vetting Investigative Standards issued by the Suitability, Credentialing, and Security Executive Agents, which expands this window of time up to sixty months using a tiered, risk-based approach of graduated levels of investigation.

IAW 5 CFR 731 and E.O. 13764, the fixed five-year periodic reinvestigation for public trust positions and national security positions will soon be eliminated and only once personnel are enrolled in a continuous vetting program. Therefore, PSD will continue the reinvestigation process until this process is completed.

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. TW 2.0 is a whole-of-government background investigation reform effort overhauling the personnel vetting process by creating a government-wide system that allows transfer of trust across organizations. All contractor employees will be subjected to the transition and will be enrolled into a continuous vetting system. 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

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 DHS on any contract and report any derogatory information concerning the individual immediately, in accordance with the contract requirements. Report this information to PSD-CEP-REPORTING@ice.dhs.gov. The report shall include the contractor employees' name and social security number, along with the adverse information being reported.

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*."

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

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.

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 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).

INFORMATION TECHNOLOGY 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 Inform

---End of Section---

OCIO/ Data Management Unit (DMU) - Data Ownership Contract Requirements Language

1. Accessibility of Government-owned Data

All stored program data associated with this acquisition shall be owned by the Government. As such, it shall be made accessible to the Government in accordance with the Minimum Data Access Capability described below. This accessibility is required to allow full data transparency, flexibility in performing data analytics, and integration with data from other government programs.

In addition to the Minimum Data Access Capability, the Government prefers, but does not require, that program data be accessible via Enhanced Access Capabilities as described below.

Definition of **"program data"**: Program Data refers to <u>any</u> data resulting from ICE and DHS organizational activity. Examples of such data include but are not limited to administrative data resulting from human resource, management, and financial actions, as well as operational data resulting from performance of the ICE mission.

Definition of "**associated with this acquisition"**: Program Data is associated with an acquisition if it is created by DHS organizational activity that is facilitated by the contractor. Examples of how a contractor might facilitate organizational activity follow:

- Program data is stored by contractor personnel
- Program data is stored by software that is managed, developed, or used by the contractor
- Program data is stored in a repository that is managed, developed, or used by the contractor

2. Minimum Data Access Capability

- The current version of all Program Data is accessible to the Government within 24 hours of request, as well as on any pre-defined schedule as required by the Government.

  Data access can occur by various means, provided that Government security requirements are met, and data is accessible in a format that is acceptable to the Government. Examples include but are not limited to APIs that are consumable by the Government, files made available for Government download (e.g., Excel Spreadsheets), or direct database query by federal or contractor personnel.

- The contractor shall format program data accessed by the Government to anticipate the maximum file size of any data to be accessed. File size shall be small enough to assure rapid processing by government applications.

- The contractor shall provide the means for the Government to interpret accessible Program Data as follows:

  - Data elements and groupings of data elements shall be clearly identifiable by labels embedded in the data itself, or by a separate schema or file layout which allows such elements and groupings to be identified.
    In the case of a relational database schema defined through Data Definition Language (DDL), data elements would be represented as columns, and groupings of data would be represented as tables. In addition, relationships between tables would be described as

foreign key relations.

- Labels or names used to identify data elements and groupings of data elements shall be approved by the Government. In addition, each label or name shall be associated with a government approved definition which describes the content of data held therein.
- Program data delivered to the Government shall conform to the Government approved definition for each data element and grouping of data elements.
- All data accessible by the Government shall be both machine readable and human-readable in plain text.
- All reference data associated with Program Data also needs to be accessible to the Government. Such reference data is required to provide complete understanding of a record.

  Reference Data Example: Program data may include a city code which uniquely identifies a city. Reference data associated with a city code may include its name, geographic boundaries, population, median income, etc. This example is provided for clarification of the meaning of reference data and may or may not apply to this specific acquisition. Examples of other reference data codes would include codes representing eye color, gender, country of origin, etc.

3. Enhanced Access Capabilities

The Government prefers that sharing of program data take place via an Application Programming Interface (API) or multiple APIs. APIs allow the Government to efficiently consume data via a widely recognized standard where the data has been completely abstracted from the technology platform that produces it.

In addition, the Government prefers that sharing of program data take place using techniques that enhance efficiency, such as Change Data Capture (CDC). CDC enhances efficiency of data transfer by providing only incremental updates to program data as opposed to providing all program data each time data is shared.

---End of Section---

PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

Limiting Access to Privacy Act and Other Sensitive Information

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at https://www.dhs.gov/system-records-notices-sorns. Applicable SORNS of other agencies may be accessed through the agencies' websites or by searching GovInfo, available at https://www.govinfo.gov that replaced the FDsys website in December 2018. SORNs may be updated at any time.

Prohibition on Performing Work Outside a Government Facility/Network/Equipment

The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall

perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

Prior Approval Required to Hire Subcontractors
The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (Subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under or relating to this contract. The Contractor (and any Subcontractor) is required to abide by Government and Agency guidance for protecting sensitive and proprietary information.

Separation Checklist for Contractor Employees
Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.

In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

As requested, contractors shall assist the ICE Point of Contact (ICE/POC), Contracting Officer, or COR with completing ICE Form 50-005/Contractor Employee Separation Clearance Checklist by returning all Government-furnished property including but not limited to computer equipment, media, credentials and passports, smart cards, mobile devices, PIV cards, calling cards, and keys and terminating access to all user accounts and systems.

Contractor's Commercial License Agreement and Government Electronic Information Rights
Except as stated in the Performance Work Statement and, where applicable, the Contractor's Commercial License Agreement, the Government Agency owns the rights to all electronic information (electronic data, electronic information systems or electronic databases) and all supporting documentation and associated metadata created as part of this contract. All deliverables (including all data and records) under the contract are the property of the U.S. Government and are considered federal records, for which the Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein. The Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

Privacy Lead Requirements
If the contract involves an IT system build or substantial development or changes to an IT system that may require privacy documentation, the Contractor shall assign or procure a Privacy Lead, to be listed under the SOW or PWS's required Contractor Personnel section. The Privacy Lead shall be responsible for providing adequate support to DHS to ensure DHS can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance. The Privacy Lead shall work with personnel from the program office, the ICE Privacy Unit, the Office of the Chief Information Officer, and the Records and Data Management Unit to ensure that the privacy documentation is kept on schedule, that

the answers to questions in the PIA are thorough and complete, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

The Privacy Lead:

- Must have excellent writing skills, the ability to explain technology clearly for a non-technical audience, and the ability to synthesize information from a variety of sources.
- Must have excellent verbal communication and organizational skills.
- Must have experience writing PIAs. Ideally the candidate would have experience writing PIAs for DHS.
- Must be knowledgeable about the Privacy Act of 1974 and the E-Government Act of 2002.
- Must be able to work well with others.

If a Privacy Lead is already in place with the program office and the contract involves IT system builds or substantial changes that may require privacy documentation, the requirement for a separate Private Lead specifically assigned under this contract may be waived provided the Contractor agrees to have the existing Privacy Lead coordinate with and support the ICE Privacy POC to ensure privacy concerns are proactively reviewed and so ICE can complete any required PTA, PIA, SORN, or other supporting documentation to support privacy compliance if required. The Contractor shall work with personnel from the program office, the ICE Office of Information Governance and Privacy, and the Office of the Chief Information Officer to ensure that the privacy documentation is kept on schedule, that the answers to questions in any privacy documents are thorough and complete, that all records management requirements are met, and that questions asked by the ICE Privacy Unit and other offices are answered in a timely fashion.

---End of Section---

A.2 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 13.3 Feb. 13, 2023 and attachments*.

A.3 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 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 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.7 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

(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 lable 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.

(End of clause)

.

Final ICE AI Contract Language

1. **Compliance with Federal Laws and Policies; AI Use Limitations.** The Contractor shall ensure any AI system or service provided complies with all applicable federal, Department of Homeland Security (DHS), and U.S. Immigration and Customs Enforcement (ICE) AI Policies, Directives, and Memos, as well as ICE AI governance requirements. The AI solution must align with the U.S. Constitution and all relevant laws and regulations, including privacy, civil rights, and civil liberties. Specifically:

    a. The Contractor must stay current and comply with any updates or new AI policy and AI governance requirements issued during the contract term.
    b. 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.
    c. 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.
    d. The contract prohibits use of AI that violates DHS policy, including:
        i. Using AI outputs as sole evidence for punitive or enforcement actions.

    ii. Utilizing AI to make or support decisions on improper bases (e.g., predicting future behavior or emotional state leading to discriminatory or unlawful actions).
  e. The Contractor must follow AI Use Case approval, Security Authorization, and ICE AI governance and AI risk management processes and requirements before developing, piloting, testing, or deploying AI in ICE environments or using ICE data.
  f. The Contractor is responsible for complying with AI Security Control Baseline requirements.

2. **Traceability, Auditability, and Transparency.** 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:
  a. Document the provenance of data used for AI training, fine-tuning, or operation.
  b. Ensure data used for AI training, fine tuning, or operation was lawfully obtained and processed.
  c. Document the provenance of any third-party AI models used (source, version, etc.).
  d. Provide comprehensive system diagrams and inventories that map the AI systems' API and system connections, data flows, and technical components.
  e. Provide comprehensive documentation explaining how the AI system works, including any models and algorithms.
  f. Ensure the AI system, where applicable, provides clear explanations or reasoning for its decisions or predictions.
  g. Ensure AI outputs are traceable, auditable, meet evidentiary standards, and are explainable to non-technical users. Additionally:
    i. Ensure GenAI inputs and their outputs are logged and preserved in line with federal, DHS, and ICE retention policies.

3. **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:
  a. 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.
  b. The Contractor must grant the Government appropriate license rights in any custom-developed AI models, software, or deliverables. Intellectual Property (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.
  c. ICE maintains ownership over and the Contractor 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.

4. **Prevention Against Vendor Lock-In:** To promote a competitive marketplace and long-term sustainability of ICE's AI capabilities, the Contractor shall:
    a. Utilize industry-standards, Application Programming Interfaces (APIs), and protocols wherever possible to ensure interoperability and combability within and between ICE and DHS systems.
    b. 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.
    c. 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.
    d. 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, derivative outputs, 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.

5. **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 Office of Management and Budget (OMB) guidance on AI risks. Key requirements include:
    a. 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.
    b. **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.

    c. **While operating the AI system:** The Contractor must re-test system performance, security, resiliency, and abuse/mis-use vulnerabilities before deploying new AI models, fine-tuned models, or other changes to AI systems that require Change Requests.

    d. **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).
        iv. Additional requirements as determined by federal, DHS, and ICE policy.

e. **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.