SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 GENERAL

The primary purpose of this contract is for teleradiology support services as outlined in Attachment 1 – Performance Work Statement (PWS). The acquisition is being conducted in accordance with (IAW) Revolutionary Federal Acquisition Regulation Overhaul (RFO) Subparts 12 (FAR Class Deviation Number 25-21) and 15 (FAR Class Deviation Number 26-08). Note, all FAR references can be found on the RFO site located at:

Revolutionary FAR Overhaul | Acquisition.GOV

B.2 CONTRACT PRICING AND CONTRACT LINE-ITEM NUMBER STRUCTURE

This is a Firm Fixed Price (FFP) contract. All Contract Line Item Numbers (CLINs) are FFP. Offerors are instructed to fill in the Contract Line Item Number (CLIN) table in Attachment 3 – Pricing Template. Attachment 3 is anticipated to be the CLIN structure that will be utilized for this contract but may be edited prior to award. Offerors may not propose an alternative CLIN structure.

B.3 MATERIALS AND EQUIPMENT

Material means property that may be consumed or expended during performance, component parts of a higher assembly, or items that lose their individual identity through incorporation into an end item. Equipment means a tangible item that is functionally complete for its intended purpose, durable, nonexpendable, and needed for performance.

After contract award, any material and equipment cost not factored into the proposed prices, and not requested by the government at any time, will not be covered under this contract.

B.4 MINIMUM AND MAXIMUM QUANTITIES

In accordance with FAR 16.504-5(b)(DEVIATION 26-04), the minimum and maximum quantity the government will acquire under this contract is as follows:

Minimum: $500,000.00 during the period of performance of the Indefinite Delivery Indefinite Quantity (IDIQ) contract. There is no additional minimum for any option periods, if exercised.

Maximum: TBD during the period of performance of the IDIQ contract. Note, the maximum for this IDIQ will be calculated based on the total proposed value of the base and all option periods multiplied by a factor of 115%. This amount will be stated in the IDIQ award as a dollar amount.

B.5 FUNDING

Funding will be obligated at the task order level. The government anticipates issuing one task order annually for the required services.

[END OF SECTION B]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION C - DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

See Attachment 1 – Performance Work Statement.

[END OF SECTION C]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION D - PACKING AND MARKING

D.1 PACKING, PACKAGING, MARKING AND STORAGE OF EQUIPMENT

Unless otherwise specified, all items to be delivered under this contract shall be preserved, packaged, and packed in accordance with normal commercial practices to meet the packing requirements of the carrier and ensure safe delivery at destination.

All packing, marking and storage incidental to shipping of equipment to be provided under this contract shall be at the contractor's expense.

D.2 SHIPPING RECEIPTS

Receipts from common carriers for shipment of materials shall be retained by the contractor and made available to the Contracting Officer (CO) upon request.

D.3 SHIPPING CONTAINER MARKINGS

All shipping containers shall be clearly marked with a delivery address.

D.4 SHIPPING INSURANCE

All shipments shall be Free on Board (FOB) destination, insured against loss or damage, and shall carry sufficient insurance to cover the full replacement value of the item(s) being shipped.

D.5 LOCATIONS

Locations are indicated in Attachment 1 – PWS, Appendix 2 – IHSC Facility Locations

[END OF SECTION D]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION E - INSPECTION AND ACCEPTANCE

E.1 CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

FAR 52.252-2 (FEB 1998)

This contract incorporates the following clauses by reference with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. Also, the full text can be accessed electronically at the following internet address:

Revolutionary FAR Overhaul | Acquisition.GOV

(End Clause)

The following clauses are incorporated by reference:

Number	Title	Date
52.246-2	Inspection of Supplies-Fixed-Price	Aug 1996
52.246-4	Inspection of Services-Fixed-Price	Aug 1996
52.246-15	Certificate of Conformance	Apr 1984

E.2 INSPECTION AND ACCEPTANCE

The government will conduct inspection and acceptance for all rendered services including deliverables. See Attachment 1 – Performance Work Statement for details.

All deliverables will be inspected for content, completeness, accuracy, and conformance to contract requirements by the Contracting Officer's Representative (COR). The scope and nature of inspections will be sufficiently comprehensive, to ensure the completeness, quality, and adequacy of all deliverables.

E.3 CONTRACTOR PERFORMANCE ASSESSMENT REPORTING SYSTEM (CPARS)

In accordance with Federal Acquisition Regulation (FAR) Subpart 42.15, it is anticipated that past performance evaluations will be entered into CPARS, the governmentwide evaluation reporting tool for all past performance reports on contracts and orders. For more information regarding CPARS, please visit http://www.cpars.gov/.

E.4 QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

Services will be evaluated in accordance with the metrics outlined in the PWS.

[END OF SECTION E]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION F - DELIVERIES OR PERFORMANCE

F.1 CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

In accordance with (IAW) FAR 52.252-2, the following clauses are incorporated by reference:

Number	Title	Date
52.242-15	Stop-Work Order	Aug 1989
52.242-17	Government Delay of Work	Apr 1984

F.2 PERIOD OF PERFORMANCE AND ORDERING PERIOD

The period of performance and ordering period of this contract is comprised of one 12 month base period, inclusive of the transition-in period, and four 12 month option periods inclusive of the transition-out period.

IDIQ Period	Term	Dates
Base	12 Months	TBD will be filled in after award
Option 1	12 Months	TBD will be filled in after award
Option 2	12 Months	TBD will be filled in after award
Option 3	12 Months	TBD will be filled in after award
Option 4	12 Months	TBD will be filled in after award

FAR clause at 52.217-8 (Option to Extend Services) will be evaluated and included in the resulting contract, allowing the government the option to extend for an additional six months at the current established rates. However, a separate CLIN will not be included.

F.3 TASK ORDER PERIOD OF PERFORMANCE AND PRICING

Task Orders (TOs) may be issued at any time during the base and/or option periods. The period of performance of any task order issued under the contract shall not exceed twelve months. TOs shall be priced using the rates provided in Section B.2 Contract Pricing And Contract Line-Item Number Structure and Section A – Solicitation/Contract Form, that will be applicable to the TO's anticipated period of performance.

F.4 PLACE OF PERFORMANCE

Addresses of each facility are found in Attachment 1, Appendix 2 – IHSC Facility Locations.

F.5 LIST OF DELIVERABLES

For a complete list of deliverables see Attachment 1 – PWS.

F.6 NOTICE OF DELAYS

In the event the contractor encounters difficulty in meeting performance requirements, or when it

anticipates difficulty in complying with the contract delivery schedule, or as soon as the contractor has knowledge that any actual or potential situation is delaying or threatens to delay the timely performance of this contract, the contractor shall immediately notify the CO and the COR in writing. This notification shall give pertinent details, and this data shall be informational only in character; this provision shall not be construed as a waiver by the government of any delivery schedule or date, or any rights or remedies provided by law or under this contract.

[END OF SECTION F]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION G - CONTRACT ADMINISTRATION DATA

G.1 CONTRACT ADMINISTRATION

The government points of contact for this resulting contract will be identified in Section A – Solicitation/Contract Form.

G.2 CONTRACTING OFFICER (CO)

The CO has the overall and primary responsibility for the administration of this contract. Only the CO has the authority to enter into, administer, modify, or terminate this contract on behalf of the government. This authority includes modifying and deviating from the contract terms, conditions, requirements, specifications, and delivery schedules; making final decisions involving such matters as invoice payments or other consideration due to the government for nonperformance or unsatisfactory performance, interpreting the contract, and resolving disputes; and terminating the contract for convenience or default. At the CO's discretion a performance requirement or performance deficiency or any other performance variation by the contractor may be waived. The contractor may submit a waiver request to the CO in writing on case-by-case basis. The CO also has authority to delegate certain responsibilities to an authorized COR who assists in the technical monitoring or administration of the contract.

G.3 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The individuals designated as the CORs for this requirement are identified in Section A – Solicitation/Contract Form. The CORs are authorized by the CO to perform specific contract administration functions such as inspection and acceptance of services and other functions of a technical nature. The CORs will represent the CO in the administration of technical details within the scope of aTask Orders (TO). The CORs are also responsible for the final inspection and acceptance of all TO deliverables and reports. The CORs are not otherwise authorized to make any representations or commitments of any kind on behalf of the CO or the Government. The CORs do not have authority to alter the contractor's obligations or to change the contract specifications, price, terms or conditions. If, as a result of technical discussions, it is desirable to modify task order obligations or the specification, changes will be issued in writing and signed by the CO.

The CO shall designate and authorize a COR as early as practicable after nomination. A copy of the letter of designation with specific duties and responsibilities will be saved to the file and available upon request.

G.4 INVOICE INSTRUCTIONS

Invoicing instructions are provided in Section A – Solicitation/Contract Form.

[END OF SECTION G]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 GENERAL PURPOSE OFFICE EQUIPMENT (GPOE) AND INFORMATION TECHNOLOGY (IT)

The contractor is expected to have the necessary facilities to meet the requirements of this contract, including any necessary General-Purpose Office Equipment (GPOE) and IT. GPOE means, but is not limited to, equipment normally found in a business office such as desks, chairs, typewriters, calculators, file cabinets, etc. "IT" means, but is not limited to, any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, movement, control, display, switching, interchange, transmission, or reception of data or information. IT includes, but is not limited to, computers, ancillary equipment, software, firmware and similar products, services (including support services), and related resources.

H.2 DISCLOSURE OF INFORMATION – CONFIDENTIAL UNCLASSIFIED INFORMATION (CUI)

Each employee of the contractor or subcontractor at any tier to whom Confidential Unclassified Information (CUI) or "Official Use Only" information may be made available or disclosed, shall be notified in writing by the contractor that Confidential Unclassified Information (CUI) or "Official Use Only" information disclosed to that individual can be used only for a purpose, and to the extent authorized herein, and that further disclosure of any such Confidential Unclassified Information (CUI) or "Official Use Only" 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. Sections 641 and 3571. Section 641 of 18 U.S.C. provides, in pertinent part, that whoever knowingly converts to his use or the use of another, or without authority sells, conveys, or disposes of any record of the United States or whoever receives the same with the intent to convert it to his use or gain, knowing it to have been converted, shall be guilty of a crime punishable by a fine or imprisoned up to 10 years, or both.

H.3 SUBCONRACTING PLAN & USE OF SUBCONRACTORS AND INDEPENDENT CONTRACTORS

The contractor is permitted to use independent contractors for services rendered under this contract. If the contractor deems it necessary to obtain the services of a subcontractor to fulfill its obligations under this contract, the contractor will notify the CO in writing of its intent to use subcontractor support for particular positions. No approval is necessary for use of a subcontractor that is a subsidiary of contractor or a subcontractor identified in the contractor's original proposal. Responsibility remains with the contractor for all subcontractor and independent contractors. Any subcontractor utilized by the contractor shall be responsible for the same requirements as the prime contractor. The contractor will remain the sole point of contact for the government in all matters related to the delivery of services under this contract.

H.4 CONTRACTORS INSURANCE

The contractor shall ensure all radiologists performing under this contractor maintain general

liability and malpractice insurance as required by industry standards. The contractor shall provide proof of insurance coverage to the CO, CS and the COR as specified in the PWS.

H.5 FACILITY ACCESS

The contractor is required to provide to the COR and the facility POCs, a list of all personnel who require access to IHSC facilities, including access during the Transition-In phase, installation of equipment, training, testing, and etcetera. All applicable contractor personnel shall be capable of passing the ICE-required building access procedures and vendor authorization in order to enter IHSC facilities. The contractor employees may be required to complete a Building Access Request Form or other documentation prior to facility access granted.

The contractor's personnel shall be required to obtain the necessary clearance required under this PWS to be granted access to the facility and its grounds. Contractor's personnel criminal history checks shall be part of the general background check for performance of services in and around the facility. This process is strictly confidential, and access to the information must be limited to the government.

H.6 CONTRACTOR EMPLOYEE IDENTIFICATION

The contractor, contractor employees, or subcontractors, shall not represent or permit itself or its employees to be represented as agents or employees of the United States government, and shall not use the names or acronyms of DHS, ICE, or Detention, Compliance, and Removals (DCR) on advertising material. The contractor shall not represent, expressly or by implication, that the services provided under this contract are endorsed by any element of the government.

All contractor personnel attending meetings, answering government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public or Congress that they are government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

H.7 DEDUCTIONS

In accordance with QASP, the government may apply financial deductions to monthly invoices as defined in the QASP. Deductions may be implemented and calculated for each category as defined in the QASP.

If the surveillance factors are below the thresholds defined in the QASP, the COR will calculate the deductions in accordance with the QASP. The deduction calculations may not be rounded. The government will notify the contractor of the total amount being deducted and provide a copy of the deductions calculation via email.

H.8 PUBLIC DISCLOSURE OF WORK UNDER THIS CONTRACT

Public disclosure of information derived from or knowledge gained as a result of work under this contract whether by press release, word of mouth, written correspondence, or any other means is prohibited without the advance written consent of the contracting officer. Any request for authority to release such information will be made in writing and submitted by the contractor to the contracting officer with a copy to the COR. Each request will be documented with sufficient evidence to justify the requested release as being in the best interest of the public. Final determination with regard to the necessity of public disclosure of such information remains solely with the contracting officer.

The prohibition against "public disclosure" is defined to include a prohibition against disclosure to any governmental agency, as well as any individual or group of individuals outside of the government.

Contractor shall insert the above, in any, and all, subcontracts hereunder relating to performance of work under this contract.

H.9 CONTRACTOR IT SECURITY ACCREDITATION

Within 6 months after contract, the contractor shall submit written proof of IT Security accreditation to DHS for approval by DHS CO. Accreditation will proceed according to the criteria of DHS Sensitive System Policy Publication, 4300A (most current version) or any replacement publication, which the CO will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the CO, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

H.10 ICE AI Contract Terms

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.

H.11 ITAR SME Cybersecurity Supply Chain Risk Management (C-SCRM)

a. Definitions:
i. Component: a unit defined by the supplier that connects to and functions as part of the product. For software products, a component is a unit of software defined by a supplier at the time the component is built, packaged, or delivered. For hardware, a component is one hardware unit designed to connect to and function as part of a larger product.
ii. End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).
iii. End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).
iv. Information and Communications Technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).
v. Product: part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.
b. Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product:
i. The contractor shall provide new equipment unless otherwise formally approved by the Government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the Government. In the event that a shipped OEM product, or part or component of that product, fails, all replacements must be new (i.e., non-refurbished, not previously used) OEM.
ii. The contractor may provide previously used OEM products only with written Government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.
c. Accounting of Components in ICT Products:
i. The contractor shall provide and maintain a list of components for each product used in performance of the contract, including through subcontracts or other arrangements. This list for

each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.

ii. The contractor shall notify the Government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to reflect the new version of the software. This includes software builds to integrate an updated component or dependency.

iii. For software products, the contractor shall provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract and replaced when End of Support (EoS) is reached.

iv. A contractor using team members in performance of the contract (e.g., subcontractors or other service providers) shall ensure that the standards for the accounting of components in this subsection are met by team members.

d. Supply-Chain Transport:

i. The contractor shall use formal, documented, and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.

ii. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance and make available for inspection upon request of the Government.

iii. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.

iv. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

v. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Changes to Ownership and Control:

The Contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any significant changes to corporate ownership or control from contract award through final delivery or the end of the period of performance. A significant change would be one in which a change occurs in the individuals or entities who, directly or indirectly, either (1) exercises substantial control over an entity, or (2) owns or controls at least 25 percent of the ownership interests of an entity.

H.12 ITAR SME Enterprise Architecture

https://usdhs.sharepoint.com/sites/dhsconnect/org/comp/mgmt/ocio/cto/Pages/ITAR·Submission

·EA·Compliance.aspx

This is a list of EA Architecture Compliance language agreed upon between Components and HQ DHS to be used in preparing SOW, PWS & SOO for IT acquisitions & services. The following Components—CBP, TSA and USCG—have their own customized version listed below that must be used. All other Components must use the DHS Enterprise Architecture Compliance language that follows.

H.13 ITAR SME FedRAMP – Cloud and 'as-a-Service'

When procuring or considering cloud services,
(a) Cloud computing. All use of cloud computing products or services that process unclassified information must comply with the FedRAMP Authorization Act, 44 U.S.C. Section 3607 et. seq. The following requirements apply when using cloud computing to provide information systems or services in the performance of the contract:

Cloud computing security requirements. The Contractor shall implement and maintain administrative, technical, and physical safeguards and controls with the security level and services required in accordance with FedRAMP Security Authorization Requirements unless notified by the Contracting Officer that this requirement has been waived by the Agency Chief Information Officer.

Cloud computing continuous monitoring. The Contractor shall maintain an adequate continuous monitoring capability based on the FedRAMP Security Authorization Requirements including processes described in the NIST Special Publication (SP) 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations and governed by the FedRAMP Continuous Monitoring Strategy Guide.

Cloud computing services cyber incident reporting. The Contractor shall report all cybersecurity incidents that are related to the cloud computing service provided under this contract. Reports shall be submitted according to FedRAMP Security Authorization Requirements, published FedRAMP Incident Communications Procedures, and Federal Incident Notification Guidelines for submitting incident notifications to CISA using the CISA incident reporting form (https://us-cert.cisa.gov/report).

H.14 ITAR SME Identity and Credentials Management (ICAM)

HSPD-12:
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.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

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.

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.

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

The DHS Office of the Chief Security Officer shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer's Representative (COR) all DHS issued Personal Identity Verification (PIV) credentials /identification cards and building passes that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or card. The Contractor or contractor personnel's failure to return all DHS issued identification cards and building passes upon expiration, upon the contractor personnel's removal from the contract, or upon demand by DHS may subject the contractor personnel and the Contractor to civil and criminal liability.

[END OF SECTION H]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION I - CONTRACT CLAUSES

I.1 NOTICE

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in this solicitation. Contracting officers will rely on representations from offers based on provisions in the solicitation. Entities are not required to, nor are they able to, update their entity registration to remove these representations in SAM.

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in agency solicitations. Examples include 52.222-25, Affirmative Action Compliance, and paragraph (d) of 52.212-3, 52.223-22, Public Disclosure of Greenhouse Gas Emissions and Reduction Goals—Representation, and Offeror Representations and Certifications—Commercial Products and Commercial Services, including paragraph (t). Additional examples include 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services, and 52.213-4, Terms and Conditions—Simplified Acquisitions (Noncommercial).

Contracting officers will not consider the following representations when making award decisions or enforcing requirements:

Paragraph (d) and (t) of 52.212-3, Offeror Representations and Certifications—Commercial Products and Commercial Services

Paragraphs (b)(33), (b)(34), (e)(1)(ix), and (e)(1)(x) of 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services. Additionally, per this deviation, in paragraph (b)(46), E.O. 14057 does not apply;

Paragraphs (e)(1)(ii)(I) and (e)(1)(ii)(J) of Alternate II of 52.212-5, Contract Terms and Conditions Required To Implement Statutes or Executive Orders—Commercial Products and Commercial Services

Paragraphs (a)(1)(vii) and (a)(1)(viii) of 52.213-4, Terms and Conditions—Simplified Acquisitions (Other Than Commercial Products and Commercial Services). Additionally, per this deviation, in paragraph (b)(1)(xvii), E.O. 14057 does not apply.

Entities are not required to update their entity registration to remove these representations in SAM.

I.2 FAR CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

In accordance with (IAW) FAR 52.252-2, the following clauses are incorporated by reference:

Number	Title	Date
52.202-1	Definitions	Jun 2020
52.203-3	Gratuities	Apr 1984
52.203-6	Restrictions on Subcontractor Sales to the Government with Alternate I	Jun 2020 Alt I Nov 2021
52.203-12	Limitation on Payments to Influence Certain Federal Transactions	Jun 2020
52.203-13	Contractor Code of Business Ethics and Conduct	Nov 2021
52.203-17	Contractor Employee Whistleblower Rights	Nov 2023
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements	Jan 2017
52.204-9	Personal Identity Verification of Contractor Personnel	Jan 2011
52.204-13	System for Award Management Maintenance with Alternate I (DEVIATION 25-19)	Aug 2025
52.204-19	Incorporation by Reference of Representations and Certifications	Dec 2014
52.207-5	Option to Purchase Equipment	Feb 1995
52.209-6	Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, Proposed for Debarment, or Voluntarily Excluded(DEVIATION 25-27)	Nov 2025
52.209-9	Updates of Publicly Available Information Regarding Responsibility Matters (DEVIATION 25-27)	Nov 2025
52.209-10	Prohibition on Contracting with Inverted Domestic Corporations (DEVIATION 25-27)	Nov 2025
52.212-4	Contract Terms and Conditions—Commercial Products and Commercial Services (DEVIATION 25-21)	Aug 2025
52.215-8	Order of Precedence-uniform Contract Format (DEVIATION 26-08)	Oct 2025
52.219-6	Notice of Total Small Business Set-Aside (DEVIATION 26-03)	Oct 2025
52.219-8	Utilization of Small Business Concerns (DEVIATION 26-03)	Oct 2025
52.219-14	Limitations on Subcontracting (DEVIATION 26-03)	Oct 2025
52.219-16	Liquidated Damages-Subcontracting Plan (DEVIATION 26-03)	Oct 2025
52.219-28	Postaward Small Business Program Rerepresentation (DEVIATION 26-03)	Oct 2025
52.222-1	Notice to the Government of Labor Disputes	Feb 1997
52.222-3	Convict Labor	Jun 2003
52.222-35	Equal Opportunity For Veterans (DEVIATION 26-10)	Oct 2025
52.222-36	Equal Opportunity for Workers with Disabilities (DEVIATION 26-10)	Oct 2025
52.222-37	Employment Reports On Veterans (DEVIATION 26-10)	Oct 2025
52.222-40	Notification of Employee Rights Under the National Labor Relations Act.	Dec 2010
52.222-50	Combating Trafficking in Persons	Nov 2021

52.222-54	Employment Eligibility Verification (DEVIATION 26-10)	Oct 2025
52.223-23	Sustainable Products and Services (DEVIATION 26-12)	Oct 2025
52.224-1	Privacy Act Notification	Apr 1984
52.224-2	Privacy Act	Apr 1984
52.224-3	Privacy Training with Alternate I*	Jan 2017 Alt I Jan 2017
52.225-1	Buy American-Supplies (DEVIATION 26-09)	Oct 2025
52.226-8	Encouraging Contractor Policies to Ban Text Messaging While Driving	May 2024
52.227-1	Authorization and Consent	Jun 2020
52.227-2	Notice and Assistance Regarding Patent and Copyright Infringement	Jun 2020
52.227-14	Rights in Data—General	May 2014
52.227-16	Additional Data Requirements	June 1987
52.227-17	Rights in Data-Special Works	Dec 2007
52.228-5	Insurance-Work on a Government Installation	Jan 1997
52.229-3	Federal, State, and Local Taxes	Feb 2013
52.229-12	Tax on Certain Foreign Procurements	Feb 2021
52.232-1	Payments	Apr 1984
52.232-8	Discounts for Prompt Payment	Feb 2002
52.232-9	Limitation on Withholding of Payments	Apr 1984
52.232-11	Extras	Apr 1984
52.232-17	Interest	May 2014
52.232-18	Availability of Funds	Apr 1984
52.232-23	Assignment of Claims	May 2014
52.232-33	Payment by Electronic Funds Transfer-System for Award Management	Oct 2018
52.232-39	Unenforceability of Unauthorized Obligations	Jun 2013
52.232-40	Providing Accelerated Payments to Small Business Subcontractors	Mar 2023
52.233-1	Disputes with Alternate I (DEVIATION 25-25)	Aug 2025
52.233-3	Protest after Award (DEVIATION 25-25)	Aug 2025
52.233-4	Applicable Law for Breach of Contract Claim (DEVIATION 25-25)	Aug 2025
52.237-2	Protection of Government Buildings, Equipment, and Vegetation	Apr 1984
52.237-3	Continuity of Services	Jan 1991
52.242-5	Payments to Small Business Subcontractors	Jan 2017
52.242-13	Bankruptcy	Jul 1995
52.243-1	Changes - Fixed-Price with Alternate I & II (DEVIATION 25-09)	Jun 2025 Alt I June 2025
52.244-6	Subcontracts for Commercial Products and Commercial Services (DEVIATION 25-34)	Sep 2025
52.245-1	Government Property Alt I	Sep 2021
52.245-9	Use and Charges	Apr 2012

52.247-5	Familiarization with Conditions	Apr 1984
52.247-15	Contractor Responsibility for Loading and Unloading	Apr 1984
52.248-1	Value Engineering	Jun 2020
52.249-2	Termination for Convenience of the Government (Fixed-Price)	Apr 2012
52.249-8	Default (Fixed-Price Supply and Service)	Apr 1984
52.253-1	Computer Generated Forms (DEVIATION 26-14)	Oct 2025

*The below deviated text is applicable to these clauses.

I.3 FAR CLAUSES AND/OR PROVISIONS INCORPORATED BY FULL TEXT

The following clauses and/or provisions are incorporated by full text.

52.216-18 Ordering (Aug 2020)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from TBD - will be filled in after award through TBD - will be filled in after award.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.

(c) A delivery order or task order is considered "issued" when—

(1) If sent by mail (includes transmittal by U.S. mail or private delivery service), the Government deposits the order in the mail;

(2) If sent by fax, the Government transmits the order to the Contractor's fax number; or

(3) If sent electronically, the Government either—

(i) Posts a copy of the delivery order or task order to a Government document access system, and notice is sent to the Contractor; or

(ii) Distributes the delivery order or task order via email to the Contractor's email address.

(d) Orders may be issued by methods other than those enumerated in this clause only if authorized in the contract.

(End of clause)

52.216-19 Order Limitations (Oct 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $154,275.00, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) Maximum order. The Contractor is not obligated to honor-

(1) Any order for a single item in excess of the maximum value of the IDIQ.;

(2) Any order for a combination of items in excess of the maximum value of the IDIQ; or

(3) A series of orders from the same ordering office within 365 days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within 5 days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of clause)

52.216-22 Indefinite Quantity (DEVIATION 26-04) (OCT 2025)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the ordering period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order, which may include order options to be exercised after the ordering period of this contract but before the end of the period of performance of the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order, including options exercised, to the same extent as if the order were completed during the contract's ordering period; provided, that the Contractor shall not be required to make any deliveries under this contract after the period of

performance end date of the IDIQ.

(End of clause)

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 1 day of contract expiration.

(End of Clause)

52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 1 day prior to the end of the performance period provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed five years.

(End of Clause)

52.222-90 Addressing DEI Discrimination by Federal Contractors (APR 2026) (DEVIATION 26-10, Revision 2)

(a) Definitions. As used in this clause—

Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (e.g., vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

(1) The Contractor will not engage in any racially discriminatory DEI activities;

(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;

(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;

(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and

(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.

(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of clause)

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 24.3).

(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)

52.237-7 Indemnification and Medical Liability Insurance (DEVIATION 26-02) (OCT 2025)

(a) It is expressly agreed and understood that this is a nonpersonal services contract, under which the professional services rendered by the Contractor are rendered in its capacity as an independent contractor. The Government may evaluate the quality of professional and administrative services provided, but retains no control over professional aspects of the services rendered, including by example, the Contractor's professional medical judgment, diagnosis, or specific medical treatments. The Contractor shall be solely liable for and expressly agrees to indemnify the Government with respect to any liability producing acts or omissions by it or by its employees or agents. The Contractor shall maintain during the term of this contract liability insurance issued by a responsible insurance carrier of not less than the following amount(s) per specialty per occurrence: $1 million per incident and $3 million per aggregate..

(b) An apparently successful offeror, upon request by the Contracting Officer, shall furnish prior to contract award evidence of its insurability concerning the medical liability insurance required by paragraph (a) of this clause.

(c) Liability insurance may be on either an occurrences basis or on a claims-made basis. If the policy is on a claims-made basis, an extended reporting endorsement (tail) for a period of not less than 3 years after the end of the contract term must also be provided.

(d) Evidence of insurance documenting the required coverage for each health care provider who will perform under this contract shall be provided to the Contracting Officer prior to the

commencement of services under this contract. If the insurance is on a claims-made basis and evidence of an extended reporting endorsement is not provided prior to the commencement of services, evidence of such endorsement shall be provided to the Contracting Officer prior to the expiration of this contract. Final payment under this contract shall be withheld until evidence of the extended reporting endorsement is provided to the Contracting Officer.

(e) The policies evidencing required insurance shall also contain an endorsement to the effect that any cancellation or material change adversely affecting the Government's interest shall not be effective until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer. If during the performance period of the contract the Contractor changes insurance providers, the Contractor must provide evidence that the Government will be indemnified to the limits specified in paragraph (a) of this clause, for the entire period of the contract, either under the new policy, or a combination of old and new policies.

(f) The Contractor shall insert the substance of this clause, including this paragraph (f), in all subcontracts under this contract for health care services and shall require such subcontractors to provide evidence of and maintain insurance in accordance with paragraph (a) of this clause. At least 5 days before the commencement of work by any subcontractor, the Contractor shall furnish to the Contracting Officer evidence of such insurance.

(End of clause)

52.240-91 Security Prohibitions and Exclusions (Aug 2025) (DEVIATION 25-23)

(a) *Definitions.* As used in this clause—
American Security Drone Act-covered foreign entity means an entity included on a list that the Federal Acquisition Security Council (FASC) develops and maintains and publishes in the System for Award Management (SAM) at https://www.sam.gov (section 1822 of Pub. L. 118-31, 41 U.S.C. 3901 note prec.).
Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).
Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.
Covered article, as defined in 41 U.S.C. 4713(k), means:
(1) Information technology, as defined in 40 U.S.C. 11101, including cloud computing services of all types;
(2) Telecommunications equipment or telecommunications service, as those terms are defined in section 3 of the Communications Act of 1934 (47 U.S.C. 153);
(3) The processing of information on a Federal or non-Federal information system, subject to the requirements of the Controlled Unclassified Information program (see 32 CFR part 2002); or
(4) Hardware, systems, devices, software, or services that include embedded or incidental information technology.
Covered foreign country means The People’s Republic of China.
Covered telecommunications equipment or services means—

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);
(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);
(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or
(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.
Critical technology means—
(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;
(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled—
(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or
(ii) For reasons relating to regional stability or surreptitious listening;
(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);
(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).
FASC-prohibited unmanned aircraft system means an unmanned aircraft system manufactured or assembled by an American Security Drone Act—covered foreign entity.
FASCSA order means any of the following orders issued under the Federal Acquisition Supply Chain Security Act (FASCSA) requiring removing covered articles from executive agency information systems or excluding one or more named sources or named covered articles from executive agency procurement actions, as described in 41 CFR 201-1.303(d) and (e):
(1) The Secretary of Homeland Security may issue FASCSA orders that apply to civilian agencies, to the extent not covered by paragraph (2) or (3) of this definition. This type of FASCSA order may be referred to as a Department of Homeland Security (DHS) FASCSA order.
(2) The Secretary of Defense may issue FASCSA orders that apply to the Department of Defense (DoD) and national security systems other than sensitive compartmented information systems. This type of FASCSA order may be referred to as a DoD FASCSA order.
(3) The Director of National Intelligence (DNI) may issue FASCSA orders that apply to the

intelligence community and sensitive compartmented information systems, to the extent not covered by paragraph (2) of this definition. This type of FASCSA order may be referred to as a DNI FASCSA order.

Information technology, as defined in 40 U.S.C. 11101(6)—

(1) Means any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use—

(i) Of that equipment; or

(ii) Of that equipment to a significant extent in the performance of a service or the furnishing of a product;

(2) Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but

(3) Does not include any equipment acquired by a Federal contractor incidental to a Federal contract.

Intelligence community, as defined by 50 U.S.C. 3003(4), means the following—

(1) The Office of the Director of National Intelligence;

(2) The Central Intelligence Agency;

(3) The National Security Agency;

(4) The Defense Intelligence Agency;

(5) The National Geospatial-Intelligence Agency;

(6) The National Reconnaissance Office;

(7) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs;

(8) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy;

(9) The Bureau of Intelligence and Research of the Department of State;

(10) The Office of Intelligence and Analysis of the Department of the Treasury;

(11) The Office of Intelligence and Analysis of the Department of Homeland Security; or

(12) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

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

Kaspersky Lab-covered article means any hardware, software, or service that—

(1) Is developed or provided by a Kaspersky Lab-covered entity;

(2) Includes any hardware, software, or service developed or provided in whole or in part by a Kaspersky Lab-covered entity; or

(3) Contains components using any hardware or software developed in whole or in part by a Kaspersky Lab-covered entity.

Kaspersky Lab-covered entity means—
(1) Kaspersky Lab;
(2) Any successor entity to Kaspersky Lab, including any change in name, e.g., "Kaspersky";
(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or
(4) Any entity of which Kaspersky Lab has a majority ownership.
National security system, as defined in 44 U.S.C. 3552, means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—
(1) The function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications); or
(2) Is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.
Sensitive compartmented information means classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.
Sensitive compartmented information system means a national security system authorized to process or store sensitive compartmented information.
Source means a non-Federal supplier, or potential supplier, of products or services, at any tier.
Subsidiary means an entity in which more than 50 percent of the entity is owned directly by a parent corporation or through another subsidiary of a parent corporation.
Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.
Unmanned aircraft means an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (49 U.S.C. 44801(11)).
Unmanned aircraft system means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the operator to operate safely and efficiently in the national airspace system (49 U.S.C. 44801(12)).
(b) *Prohibitions on providing or using specific products or services in performance of contract*. Unless a waiver or exception applies, the Contractor is prohibited from providing any products or services to the Government or using in the performance of the contract any of the following:
(1) A covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees (section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328));
(2) A Kaspersky Lab-covered article (Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91));
(3) Covered telecommunications equipment or services used as a substantial or essential

component of any system, or as critical technology as part of any system (paragraphs (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)). This does not prohibit contractors from providing—
(i) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or
(ii) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.
(c) Prohibition on unmanned aircraft systems manufactured or assembled by American Security Drone Act—covered foreign entities.
(1) Prohibition. The Contractor is prohibited from—
(i) Delivering any FASC-prohibited unmanned aircraft system, which includes unmanned aircraft (i.e., drones) and associated elements (sections 1823 and 1826 of American Security Drone Act of 2023, within the National Defense Authorization Act for Fiscal Year 2024, Pub. L. 118-31, Div. A, Title XVIII, Subtitle B, 41 U.S.C. 3901 note prec.);
(ii) On or after December 22, 2025, operating a FASC-prohibited unmanned aircraft system in the performance of the contract (section 1824 of Pub. L. 118-31); and
(iii) On or after December 22, 2025, using Federal funds to procure or operate a FASC-prohibited unmanned aircraft system (section 1825 of Pub. L. 118-31).
(2) *Procedures*. The Contractor shall search SAM for the FASC-maintained list of American Security Drone Act—covered foreign entities before proposing, or using in performance of the contract, any unmanned aircraft system. Also, the Contractor shall ensure any effort or expenditure associated with a FASC-prohibited unmanned aircraft system is consistent with a corresponding exemption, exception, or waiver determination expressly stated in the contract.
(3) *Exemptions, exceptions, and waivers*. The prohibitions in paragraph (c) of this clause do not apply where the agency has determined an exemption, exception, or waiver applies, and the contract indicates that such a determination has been made. See sections 1823 through 1825 and 1832 of Public Law 118-31 for statutory requirements pertaining to exemptions, exceptions, and waivers.
(d) *Prohibition on using or providing specific products or services or conducting certain transactions regardless of connection to contract*.
(1) *Certain telecommunications and video surveillance equipment, systems, or services*.
(i) Unless an applicable waiver has been issued by the Government, the Contractor cannot use any equipment, systems, or services that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system (paragraph (a)(1)(B) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232)).
(ii) This prohibition applies to using covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. This does not prohibit the contractor from using—
(A) A service that connects to the facilities of a third party, such as backhaul, roaming, or interconnection arrangements; or
(B) Telecommunications equipment that cannot route or redirect user data traffic or cannot permit visibility into any user data or packets that such equipment transmits or otherwise handles.
(2) *Office of Foreign Assets Control Restrictions*.

(i) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.
(ii) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas.
(A) For lists of entities and individuals subject to economic sanctions, see OFAC's List of Specially Designated Nationals and Blocked Persons at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.
(B) For more information about these restrictions, as well as updates, see OFAC's regulations at 31 CFR chapter V and at https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information.
(C) To conduct electronic screens of potential parties to regulated transactions, see the consolidated screening list at https://www.trade.gov/consolidated-screening-list, which consolidates multiple export screening lists of the Departments of Commerce, State, and the Treasury.
(3) *Sudan prohibition*. The Contractor is prohibited from conducting any restricted business operations in Sudan in accordance with Accountability and Divestment Act of 2007 (Pub. L. 110-174).
(4) *Iran prohibitions*.
(i) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, the contractor shall not engage in certain activities or transactions relating to Iran (section 6(b)(1)(A) of Iran Sanctions Act (50 U.S.C. 1701 note).
(ii) Unless an exception applies according to paragraph (d)(4)(iii) or the Government grants a waiver, contractor shall not export certain sensitive technology to Iran, as determined by the President, and has an active exclusion in SAM (22 U.S.C. 8515).
(iii) The prohibition in paragraphs (d)(4)(i) and (d)(4)(ii) do not apply if the acquisition is subject to trade agreements and the offeror certifies that all the offered products are designated country end products or designated country construction material (see part 25).
(iv) Unless an exception applies or the Government grants a waiver, contractors are prohibited from knowingly engaging in any significant transaction (i.e., over $15,000) with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked according to the International Emergency Economic Powers Act (section 6(b)(1)(B) of Iran Sanctions Act (50 U.S.C. 1701 note)).
(e) *Governmentwide exclusion and removal orders*.
(1) Unless the Government has issued an applicable waiver, contractors shall not provide or use as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order as follows:
(i) For solicitations and contracts awarded by a Department of Defense contracting office, DoD FASCSA orders apply.
(ii) For all other solicitations and contracts, DHS FASCSA orders apply.
(2) The Contractor shall search for the phrase "FASCSA order" in the System for Award

Management (SAM) at https://www.sam.gov to locate applicable FASCSA orders.
(3) The Government may identify in the solicitation other FASCSA orders that are not in SAM, which are effective and apply to the solicitation and resulting contract.
(4) A FASCSA order issued after the date of solicitation applies to this contract only if added by an amendment to the solicitation or modification to the contract (see FAR 40.204-1(c)).
(f) *Reasonable inquiry*. The contractor shall conduct a reasonable inquiry to determine if there are any prohibited products or services. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.
(g) *Removal of prohibited products and services*. For Federal Supply Schedules, Governmentwide acquisition contracts, multi-agency contracts or any other procurement instrument intended for use by multiple agencies, upon notification from the Contracting Officer, during the performance of the contract, the Contractor shall promptly make any necessary changes or modifications to remove any product or service produced or provided by a source that this clause prohibits.
(h) *General report*.
(1) If the Contractor identifies or is notified by any source, (including a subcontractor at any tier), that any product or service provided or used (or to be provided or used) during contract performance does not comply with any prohibition in this clause, then the Contractor shall report the following information, or as much information is known, in writing to the contracting office as identified in paragraph (h)(2) within 72 hours:
(i) Contract number and order number, if applicable;
(ii) The specific prohibition the product or service is not complying with;
(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);
(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));
(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;
(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the contractor would like the Government to consider a waiver, and asks for such a waiver);
(vii) Whether alternative products or services are available that would comply with the prohibition;
(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:
(A) Brand;
(B) Model number, OEM number, manufacturer part number, or wholesaler number; and
(C) Item description, as applicable.
(ix) Any readily available information about mitigation actions implemented or recommended.
(2) If a report must be submitted to a contracting office, the Contractor shall submit the report as follows:
(i) If a Department of Defense contracting office, the Contractor shall report to the website

at https://dibnet.dod.mil.
(ii) For all other contracting offices, the Contractor shall report to the Contracting Officer.
(iii) For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order.
(3) If the report provided does not contain any of the information required by paragraph (h)(1) of this clause, and the contractor later discovers new information that is required by paragraph (h)(1) of this clause, then the contractor shall submit a subsequent report within 72 hours of discovering the new information.
(4) The contractor shall also report the information in paragraph (h)(1) if the contractor wishes to ask for a waiver of the requirements of a new FASCSA order being applied through modification.
(i) *New FASCSA orders report*.
(1) During contract performance, the Contractor shall review SAM at least once every three months, or as advised by the Contracting Officer, to check for covered articles subject to FASCSA order(s), or for products or services produced by a source subject to FASCSA order(s) not currently identified under paragraph (e) of this clause.
(2) If the Contractor identifies a new FASCSA order(s) that could impact their supply chain, then the Contractor shall conduct a reasonable inquiry to identify whether a covered article or product or service produced or provided by a source subject to the FASCSA order(s) was provided to the Government or used during contract performance. The inquiry will look at any information in the entity's possession but does not need to include an internal or third-party audit.
(3) The Contractor shall submit a report to the contracting office identified in paragraph (h)(2) of this clause if the Contractor identifies, including through any notification by a subcontractor at any tier, that a covered article or product or service produced or provided by a source was provided to the Government or used during contract performance and is subject to a FASCSA order(s). For indefinite delivery contracts, the Contractor shall report to both the contracting office for the indefinite delivery contract and the contracting office for any affected order. The Contractor shall report the following information within 72 hours for each covered article or each product or service produced or provided by a source, where the covered article or source is subject to a FASCSA order:
(i) Contract number and order number, if applicable;
(ii) Name of the covered article or source subject to a FASCSA order;
(iii) The specific FASCSA order the product or service does not comply with;
(iv) The elements of (h)(1)(iii) through (ix) of this clause.
(j) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (j) but excluding subparagraphs (d)(1) and (i)(1), in all subcontracts and other contractual instruments, including subcontracts for acquiring commercial products or commercial services.

(End of clause)

52.240-93 Basic Safeguarding of Covered Contractor Information Systems (Aug 2025) (DEVIATION 25-23)

(a) Definitions. As used in this clause—
Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information—
(1) Means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government; but
(2) Does not include information provided by the Government to the public (such as on public websites) or simple transactional information (such as information necessary to process payments).
Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).
Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).
Safeguarding means measures or controls that are prescribed to protect information systems.
(b) *Safeguarding requirements*.
(1) Basic requirements. The Contractor shall safeguard its covered contractor information systems by implementing, at minimum, the following security controls:
(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
(iii) Verify and control/limit connections to and use of external information systems.
(iv) Control information posted or processed on publicly accessible information systems.
(v) Identify information system users, processes acting on behalf of users, or devices.
(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.
(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.
(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.
(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.
(xii) Identify, report, and correct information and information system flaws in a timely manner.
(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
(xiv) Update malicious code protection mechanisms when new releases are available.
(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.
(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal departments and agencies relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial products, other than commercially available off-the-shelf items, or commercial services), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

(End of clause)

52.252-6 Authorized Deviations In Clauses (NOV 2020)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.
(b) The use in this solicitation or contract of any FAR clause or Homeland Security Acquisition Regulation (48 CFR Chapter 30) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of Clause)

HSAM/HSAR CLAUSES AND/OR PROVISIONS INCORPORATED BY REFERENCE

Number	Title(s)	DATE
3052.225-70	Requirement for Use of Certain Domestic Commodities	Nov 2024

3052.212-70 Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (July 2023) (HSAR DEVIATION 25-09)

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:

(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.
X 3052.247-72 F.o.B. Destination Only.

(b) Clauses.

X 3052.203-70 Instructions for Contractor Disclosure of Violations.
X 3052.205-70 Advertisement, Publicizing Awards, and Releases.
X Alternate I
____3052.209-72 Organizational Conflicts of Interest.
____3052.209-73 Limitation on Future Contracting.
X 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.
X 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.
X 3052.240-71 Contractor Employee Access.
X Alternate I
____Alternate II
X 3052.240-72 Safeguarding of Controlled Unclassified Information.
X Alternate I
X 3052.240-73 Notification and Credit Monitoring Requirements for Personally Identifiable Information Incidents.
X 3052.242-72 Contracting Officer's Representative.
____3052.249-90 Contract Termination. (USCG) (End of clause)

(End of clause)

HSAM/HSAR CLAUSES AND/OR PROVISIONS INCORPORATED BY FULL TEXT

3052.209-70 Prohibition on Contracts with Corporate Expatriates (Jun 2006)

(a) Prohibitions.
Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an

inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation means a foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)—

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) Certain stock disregarded. For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) Plan deemed in certain cases. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) Certain transfers disregarded. The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) Special rule for related partnerships. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the

meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.
(e) Treatment of Certain Rights.
(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:
(i) warrants;
(ii) options;
(iii) contracts to acquire stock;
(iv) convertible debt instruments; and
(v) other similar interests.
(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.
(f) Disclosure. The Offeror under this solicitation represents that [Check one]:

it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003;

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it has submitted a request for waiver pursuant to 3009.108-7004, which has not been denied; or

it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.108-7001 through 3009.108-7003, but it plans to submit a request for waiver pursuant to 3009.108-7004.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of Clause)

3052.215-70 Key personnel or facilities (Dec 2003)

(a) The personnel or facilities specified below are considered essential to the work being performed under this contract and may, with the consent of the contracting parties, be changed from time to time during the course of the contract by adding or deleting personnel or facilities, as appropriate. (b) Before removing or replacing any of the specified individuals or facilities, the Contractor shall notify the Contracting Officer, in writing, before the change becomes effective. The Contractor shall submit sufficient information to support the proposed action and to enable the Contracting Officer to evaluate the potential impact of the change on this contract. The Contractor shall not remove or replace personnel or facilities until the Contracting Officer approves the change.

The Key Personnel or Facilities under this Contract:

Project Manager

(End of clause)

3052.240-71 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.

Alternate I (JULY 2023)

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

(End of clause)

3052.240-72 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.

Alternate I (JULY 2023)

(a) *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 13.3, February 13, 2023), 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 2015 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)

3052.240-73 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)

3052.222-70 Strikes Or Picketing Affecting Timely Completion Of The Contract Work (DEC 2003)

Notwithstanding any other provision hereof, the Contractor is responsible for delays arising out of labor disputes, including but not limited to strikes, if such strikes are reasonably avoidable. A delay caused by a strike or by picketing which constitutes an unfair labor practice is not excusable unless the Contractor takes all reasonable and appropriate action to end such a strike or picketing, such as the filing of a charge with the National Labor Relations Board, the use of other available Government procedures, and the use of private boards or organizations for the settlement of disputes.

(End of clause)

3052.222-71 Strikes Or Picketing Affecting Access To A Dhs Facility (DEC 2003)

If the Contracting Officer notifies the Contractor in writing that a strike or picketing: (a) is directed at the Contractor or subcontractor or any employee of either; and (b) impedes or threatens to impede access by any person to a DHS facility where the site of the work is located, the Contractor shall take all appropriate action to end such strike or picketing, including, if necessary, the filing of a charge of unfair labor practice with the National Labor Relations Board or the use of other available judicial or administrative remedies.

(End of clause)

Special Clause Information Technology Security Awareness Training (JULY 2023)

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

Security Training Requirements.

All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part

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

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

[END OF SECTION I]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION J - LIST OF ATTACHMENTS

The following is a list of all attachments associated with this requirement.

Attachments	
Attachment 1	Performance Work Statement (PWS)
- Appendix 1	IHSC Facility Locations
- Appendix 2	X-Ray Historical Data FY2024 Thru FY2025
- Appendix 3	Appendix 3 - Chest X-Ray Templates
Attachment 2	Past Performance and Experience Form
Attachment 3	Pricing Template
Attachment 4	Question Template

[END OF SECTION J]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION K - REPRESENTATIONS, CERTIFICATIONS, AND OTHER STATEMENTS OF OFFERORS OR RESPONDENTS

K.1 PROVISIONS INCORPORATED BY REFERENCE

FAR 52.252-1 Solicitation Provisions Incorporated by Reference (Feb 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. The contractor is cautioned that the listed provisions may include blocks that must be completed by the contractor and submitted with its proposal or offer. In lieu of submitting the full text of those provisions, the contractor may identify the provision by paragraph identifier and provide the appropriate information with its proposal or offer. Also, the full text of a solicitation provision may be accessed electronically at this address:

https://www.acquisition.gov/far/

(End Provision)

Number	Title	Date
52.203-11	Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions	Sep 2024
52.203-18	Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements - Representation	Jan 2017
52.209-2	Prohibition on Contracting with Inverted Domestic Corporations-Representation (DEVIATION 25-27)	Nov 2025
52.229-11	Tax on Certain Foreign Procurements—Notice and Representation	June 2020

K.2 PROVISIONS INCORPORATED IN FULL TEXT

52.203-2 Certificate of Independent Price Determination (Apr 1985)

(a) The offeror certifies that-

(1) The prices in this offer have been arrived at independently, without, for the purpose of restricting competition, any consultation, communication, or agreement with any other offeror or competitor relating to-

(i) Those prices;

(ii) The intention to submit an offer; or

(iii) The methods or factors used to calculate the prices offered.

(2) The prices in this offer have not been and will not be knowingly disclosed by the offeror, directly or indirectly, to any other offeror or competitor before bid opening (in the case of a sealed bid solicitation) or contract award (in the case of a negotiated solicitation) unless otherwise required by law; and

(3) No attempt has been made or will be made by the offeror to induce any other concern to submit or not to submit an offer for the purpose of restricting competition.

(b) Each signature on the offer is considered to be a certification by the signatory that the signatory-

(1) Is the person in the offeror's organization responsible for determining the prices being offered in this bid or proposal, and that the signatory has not participated and will not participate in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; or

(2)(i) Has been authorized, in writing, to act as agent for the following principals in certifying that those principals have not participated, and will not participate in any action contrary to paragraphs (a)(1) through (a)(3) of this provision _____ **[insert full name of person(s) in the offeror's organization responsible for determining the prices offered in this bid or proposal, and the title of his or her position in the offeror's organization];**
(ii) As an authorized agent, does certify that the principals named in subdivision (b)(2)(i) of this provision have not participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision; and

(iii) As an agent, has not personally participated, and will not participate, in any action contrary to paragraphs (a)(1) through (a)(3) of this provision.

(c) If the offeror deletes or modifies subparagraph (a)(2) above, the offeror must furnish with its offer a signed statement setting forth in detail the circumstances of the disclosure.

(End of provision)

52.209-5 Certification Regarding Responsibility Matters (Nov 2025)(DEVIATION 25-27)

(a)(1) The Offeror certifies, to the best of its knowledge and belief, that—
(i) The Offeror and/or any of its Principals—

(A) **Are □ are not □** presently debarred, suspended, proposed for debarment, or declared ineligible for the award of contracts by any Federal agency;
(B) **Have □ have not □**, within a three-year period preceding this offer, been convicted of or had a civil judgment rendered against them for: commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or local) contract or subcontract; violation of Federal or State antitrust statutes relating to the submission of offers; or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, violating Federal criminal tax laws, or receiving stolen property (if offeror checks "have",

the offeror shall also see 52.209-7, if included in this solicitation);
(C) **Are □ are not □** presently indicted for, or otherwise criminally or civilly charged by a governmental entity with, commission of any of the offenses enumerated in paragraph (a)(1)(i)(B) of this provision; and

(D) **Have □, have not □,** within a three-year period preceding this offer, been notified of any delinquent Federal taxes in an amount that exceeds the threshold at 9.104-5(a)(2) for which the liability remains unsatisfied. Federal taxes are considered delinquent if both of the following criteria apply:

(1) The tax liability is finally determined. The liability is finally determined if it has been assessed. A liability is not finally determined if a pending administrative or judicial challenge remains. In the case of a judicial challenge to the liability, the liability is not finally determined until all judicial appeal rights have been exhausted.

(2) The taxpayer is delinquent in making payment. A taxpayer is delinquent if the taxpayer has failed to pay the tax liability when full payment was due and required. A taxpayer is not delinquent in cases where enforced collection action is precluded.

(ii) The Offeror has □ has not □, within a 3-year period preceding this offer, had one or more contracts terminated for default by any Federal agency.

(2) "Principal," for the purposes of this certification, means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The Offeror shall provide immediate written notice to the Contracting Officer if, at any time prior to contract award, the Offeror learns that its certification was erroneous when submitted or has become erroneous by reason of changed circumstances.

(c) A certification that any of the items in paragraph (a) of this provision exists will not necessarily result in withholding of an award under this solicitation. However, the Government will consider the certification in connection with a determination of the Offeror's responsibility. Failure of the Offeror to furnish a certification or provide such additional information as requested by the Contracting Officer may render the Offeror nonresponsible.

(d) This provision does not require establishment of a system of records in order to render, in good faith, the certification required by paragraph (a). The knowledge and information of an Offeror is not required to exceed that which is normally possessed by a prudent person in the ordinary course of business dealings.

(e) The certification in paragraph (a) of this provision is a material representation of fact upon which reliance was placed when making award. If the Government later determines that the Offeror knowingly rendered an erroneous certification, in addition to other remedies available to the Government, the Contracting Officer may terminate the contract resulting from this solicitation for default.

(End of provision)

52.209-7 Information Regarding Responsibility Matters (Nov 2025) (DEVIATION 25-27)

(a) Definitions. As used in this provision—

Administrative proceeding means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

Federal contracts and grants with total value greater than $10,000,000 means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

Principal means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror □ **has** □ **does no**t have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in–

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of

$100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management, which can be accessed via https://www.sam.gov (see 52.204-7).

(End of provision)

52.209-11 Representation by Corporations Regarding Delinquent Tax Liability or a Felony Conviction under any Federal Law (Nov 2025) (DEVIATION 25-27)

(a) The Government will not enter into a contract with any corporation that—

(1) Has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, where the awarding agency is aware of the unpaid tax liability, unless an agency has considered suspension or debarment of the corporation and made a determination that suspension or debarment is not necessary to protect the interests of the Government; or

(2) Was convicted of a felony criminal violation under any Federal law within the preceding 24 months, where the awarding agency is aware of the conviction, unless an agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government.

(b) The Offeror represents that–

(1) **It is □ is not □** a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability; and

(2) **It is □ is not □** a corporation that was convicted of a felony criminal violation under a Federal law within the preceding 24 months.

(End of provision)

52.212-2 Evaluation—Commercial Products and Commercial Services (DEVIATION 25-21) (Aug 2025)

(a) Evaluation factors. The Government will award a contract resulting from this solicitation to the responsible Offeror whose offer conforming to the solicitation will be most advantageous to the Government, price and other factors considered. The following factors will be used to evaluate offers:

See RFP Section M.

(b) *Options (if applicable)*. The Government will evaluate offers for award purposes by adding the total price for all options to the total price for the basic requirement. The Government may determine that an offer is unacceptable if the option prices are significantly unbalanced. The evaluation of options does not obligate the Government to exercise the option(s).

(c) *Notice of award*. A written notice of award or acceptance of an offer furnished to the successful Offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

(End of provision)

52.219-1 Small Business Program Representations (DEVIATION 26-03) (Oct 2025)

(a) Definitions. As used in this provision-

Economically disadvantaged women-owned small business (EDWOSB) concern means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States and who are economically disadvantaged in accordance with 13 CFR part 127, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300. It automatically qualifies as a women-owned small business concern eligible under the WOSB Program.

HUBZone small business concern means a small business concern that meets the requirements described in 13 CFR 126.200, is certified by the Small Business Administration (SBA) and designated by SBA as a HUBZone small business concern in the Small Business Search (SBS) (13 CFR 126.103).

Service-disabled veteran-owned small business (SDVOSB) concern eligible under the SDVOSB Program means an SDVOSB concern that is designated in the System for Award Management (SAM) as certified by the Small Business Administration (SBA) in accordance with 13 CFR 128.300.

Small business concern—

(1) Means a concern, including its affiliates, that is independently owned and operated, not dominant in its field of operation, and qualified as a small business under the criteria in 13 CFR part 121 and the size standard in paragraph (b) of this provision.

(2) Affiliates, as used in this definition, means business concerns, one of whom directly or indirectly controls or has the power to control the others, or a third party or parties control or have the power to control the others. In determining whether affiliation exists, consideration is given to all appropriate factors including common ownership, common management, and contractual relationships. SBA determines affiliation based on the factors set forth at 13 CFR 121.103.

Small disadvantaged business concern means a small business concern that-

(1) Is at least 51 percent unconditionally and directly owned (as defined at 13 CFR 124.105) by one or more socially disadvantaged (as defined at 13 CFR 124.103) and economically disadvantaged (as defined at 13 CFR 124.104) individuals who are citizens of the United States, and

(2) The management and daily business operations of which are controlled (as defined at 13 CFR 124.106) by individuals who meet the criteria in paragraph (1) of this definition.

Women-owned small business (WOSB) concern eligible under the WOSB Program (in accordance with 13 CFR part 127) means a small business concern that is at least 51 percent directly and unconditionally owned by, and the management and daily business operations of which are controlled by, one or more women who are citizens of the United States, and the concern is certified by SBA or an approved third-party certifier in accordance with 13 CFR 127.300.

(b)(1) The North American Industry Classification System (NAICS) code for this acquisition is **621512 - Diagnostic Imaging Centers**.

(2) The small business size standard is **$19M**.

(3) The small business size standard for a concern that submits an offer, other than on a construction or service acquisition, but proposes to furnish an end item that it did not itself manufacture, process, or produce (i.e., nonmanufacturer), is 500 employees, or 150 employees for information technology value-added resellers under NAICS code 541519, if the acquisition—

(i) Is set aside for small business and has a value above the simplified acquisition threshold;

(ii) Uses the HUBZone price evaluation preference regardless of dollar value, unless the offeror waives the price evaluation preference; or

(iii) Is an 8(a), HUBZone, service-disabled veteran-owned, economically disadvantaged women-owned, or women-owned small business set-aside or sole-source award regardless of dollar value.

(c) Representations.(1) The offeror represents as part of its offer that—
(i) **it □ is, □ is not** a small business concern; or

(ii) **It □ is, □ is not** a small business joint venture that complies with the requirements of 13 CFR 121.103(h) and 13 CFR 125.8(a) and (b). **[The offeror shall enter the name and unique entity identifier of each party to the joint venture: __.]**

(2) **[Complete only if the offeror represented itself as a small business concern in paragraph (c)(1) of this provision.]** The offeror represents that **it □ is, □ is not** a women-owned small disadvantage business concern.

(3) Women-owned small business (WOSB) joint venture eligible under the WOSB Program. The offeror represents as part of its offer that **it □ is, □ is not** a joint venture that complies with the requirements of 13 CFR 127.506(a) through (c). **[The offeror shall enter the name and unique entity identifier of each party to the joint venture: __.]**

(4) Economically disadvantaged women-owned small business (EDWOSB) joint venture. The offeror represents as part of its offer that **it □ is, □ is not** a joint venture that complies with the requirements of 13 CFR 127.506(a) through (c). **[The offeror shall enter the name and unique entity identifier of each party to the joint venture: __.]**

(5) SDVOSB joint venture eligible under the SDVOSB Program. **[Complete only if the offeror is certified as a SDVOSB concern].** The offeror represents as part of its offer that **it □ is, □ is not** a SDVOSB joint venture eligible under the SDVOSB Program that complies with the requirements of 13 CFR 128.402. **[The offeror shall enter the name and unique entity identifier of each party to the joint venture:__.]**

(6) HUBZone joint venture eligible under the HUBZone Program. **[Complete only if the offeror is a HUBZone small business concern.]** The offeror represents, as part of its offer, that **it □ is, □ is not** a HUBZone joint venture that complies with the requirements of 13 CFR 126.616(a) through (c). **[The offeror shall enter the name and unique entity identifier of each party to the joint venture: __.]** Each HUBZone small business concern participating in the HUBZone joint venture must be certified as a HUBZone concern.

(d) Notice. Under 15 U.S.C. 645(d), any person who misrepresents a firm's status as a business concern that is small, HUBZone small, small disadvantaged, service-disabled veteran-owned small, economically disadvantaged women-owned small, or women-owned small eligible under the WOSB Program in order to obtain a contract to be awarded under the preference programs established pursuant to section 8, 9, 15, 31, and 36 of the Small Business Act or any other provision of Federal law that specifically references section 8(d) for a definition of program eligibility, will be—

(1) Punished by imposition of fine, imprisonment, or both;

(2) Subject to administrative remedies, including suspension and debarment; and

(3) Ineligible for participation in programs conducted under the authority of the Act.

(End of provision)

52.225-2 Buy American Certificate (Oct 2022)

(a)(1) The Offeror certifies that each end product, except those listed in paragraph (b) of this provision, is a domestic end product and that each domestic end product listed in paragraph (c) of this provision contains a critical component.
(2) The Offeror shall list as foreign end products those end products manufactured in the United States that do not qualify as domestic end products. For those foreign end products that do not consist wholly or predominantly of iron or steel or a combination of both, the Offeror shall also indicate whether these foreign end products exceed 55 percent domestic content, except for those that are COTS items. If the percentage of the domestic content is unknown, select "no".

(3) The Offeror shall separately list the line item numbers of domestic end products that contain a critical component (see FAR 25.105).

(4) The terms "commercially available off-the-shelf (COTS) item," "critical component," "domestic end product," "end product," and "foreign end product" are defined in the clause of this solicitation entitled "Buy American-Supplies."

(b) Foreign End Products:

Line Item No. Country of origin Exceeds 55% domestic content (yes/no)

(b)[List as necessary]

(c) Domestic end products containing a critical component:

Line Item No. ___

[List as necessary]

(d) The Government will evaluate offers in accordance with the policies and procedures of part 25 of the Federal Acquisition Regulation.

(End of provision)

52.240-90 Security Prohibitions and Exclusions Representations and Certifications (Aug 2025) (DEVIATION 25-23)

(a) Definitions. As used in this provision-—

Backhaul, covered article, covered telecommunications equipment or services, critical technology,

FASCSA order, Intelligence community, interconnection arrangements, national security system, roaming, sensitive compartmented information, sensitive compartmented information system, source, and substantial or essential component have the meanings provided in the clause 52.240-91, Security Prohibitions and Exclusions.

Business operations means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.

Marginalized populations of Sudan means—

(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and

(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted under specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

Sensitive technology—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

(b) Procedures.

(1) Covered telecommunications and video surveillance. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at https://www.sam.gov for entities excluded from receiving federal awards for "covered telecommunications equipment or services."

(2) FASCSA Orders.

(i) The Offeror shall search in SAM for the phrase "FASCSA order" for any covered article, or any products or services produced or provided by a source, if there is an applicable FASCSA order described in paragraph (e) of FAR 52.240-91, Security Prohibitions and Exclusions.

(ii) The Offeror shall review the solicitation for any FASCSA orders that are not in SAM but are effective and apply to the solicitation and resultant contract (see FAR 40.204-1(c)(2)).

(iii) FASCSA orders issued after the date of solicitation do not apply unless added by an amendment to the solicitation.

(c) Covered telecommunications equipment or services representations. By submission of its offer, the Offeror represents that, after conducting a reasonable inquiry (that looks at any information in the Offeror's possession but does not need to include an internal or third-party audit)—

(1) It will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation, except as waived by the solicitation, or as disclosed in paragraph (g); and

(2) It does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services, except as waived by the solicitation, or as disclosed in paragraph (g).

(d) FASCSA Representation. By submission of this offer, the offeror represents that it has conducted a reasonable inquiry, and that the offeror does not propose to provide or use in response to this solicitation any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order in effect on the date the solicitation was issued, except as waived by the solicitation, or as disclosed in paragraph (g). A reasonable inquiry will look at any information in the offeror's possession but does not need to include an internal or third-party audit.

(e) Sudan certification. By submission of its offer, the offeror certifies, after conducting a

reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), that the offeror does not conduct any restricted business operations in Sudan.

(f) Iran Representation and Certifications.

(1) Except as provided in paragraph (f)(2) of this provision or if a waiver has been granted in accordance with FAR 40.203-3, the offeror, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), by submission of its offer—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person (as defined at section 15 of the Iran Sanctions Act of 1996, Pub. L. 104-172, 50 U.S.C. 1701 note) owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Act. These sanctioned activities are in the areas of development of the petroleum resources of Iran, production of refined petroleum products in Iran, sale and provision of refined petroleum products to Iran, and contributing to Iran's ability to acquire or develop certain weapons or technologies; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $15,000 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx)

(2) Exception for trade agreements. The representation and certification requirements of paragraph (f)(1) of this provision do not apply if—

(i) This solicitation includes a trade agreements notice or certification (e.g., 52.225-6, Trade Agreements Certificate); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products or designated country construction material.

(iii) The offeror shall email questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(g) Disclosure.

(1) If the Offeror is not able to represent compliance with the prohibitions in paragraphs (c) or (d), then the Offeror shall disclose within 72 hours to the contracting office identified in paragraph (g)(2) the following information for each product or service not compliant:

(i) Contract number and order number, if applicable;

(ii) Identification of whether this disclosure relates to paragraph (c) on covered telecommunication equipment or services, or to paragraph (d) on FASCSA orders;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication, assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the offeror would like the Government to consider a waiver);

(vii) Whether alternative products or services are available that would be compliant with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions undertaken or recommended.

(2) If a disclosure is required to be submitted to a contracting office, the offeror shall submit the disclosure as follows:

(i) If a Department of Defense contracting office, the offeror shall submit the disclosure to the website at https://dibnet.dod.mil.

(ii) For all other contracting offices, the Offeror shall submit the disclosure to the Contracting Officer.

(3) If the disclosure provided does not contain any of the information required by paragraph (1),

and the Offeror later discovers new information that is required by paragraph (1), then the Offeror shall submit a subsequent disclosure within 72 hours of discovering the new information.

(h) Executive agency review of disclosures. The Contracting Officer will review disclosures provided in paragraph (g) to determine if any applicable waiver may be sought. The Contracting Officer may choose not to pursue a waiver and may instead make an award to an Offeror that does not require a waiver.

(End of provision)

[END OF SECTION K]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION L - INSTRUCTIONS, CONDITION, AND NOTICES TO CONTRACTORS

L.1 FAR PROVISIONS INCORPORATED BY REFERENCE

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make their full text available. The contractor is cautioned that the listed provisions may include blocks that must be completed by the contractor and submitted with its proposal or offer. In lieu of submitting the full text of those provisions, the contractor may identify the provision by paragraph identifier and provide the appropriate information with its proposal or offer. Also, the full text of a solicitation provision may be accessed electronically at this address:

Revolutionary FAR Overhaul | Acquisition.GOV

Number	Title	Date
52.204-7	System for Award Management (DEVIATION 25-19)	Aug 2025
52.212-1	Instructions to Offerors—Commercial Products and Commercial Services (DEVIATION 25-21)	Aug 2025
52.215-1	Instructions to Offerors—Competitive Acquisition (DEVIATION 26-08)	Oct 2025

L.2 FAR PROVISIONS INCORPORATED IN FULL TEXT

52.233-2 Service of Protest (AUG 2025) (DEVIATION 25-25)

(a) Protests, (as defined in FAR 33.102), that are filed directly with an agency, and copies of any protests that are filed with the Government Accountability Office (GAO), must be served on the Contracting Officer identified in the solicitation by obtaining written and dated acknowledgment of receipt from them.

(b) The copy of any protest must be received in the office designated above within one day of filing a protest with the GAO.

(End of provision)

52.252-5 Authorized Deviations in Provisions (Nov 2020)

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR Chapter 1) provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the provision.

(b) The use in this solicitation of any FAR clause or Homeland Security Acquisition Regulation (48 CFR Chapter 30) clause with an authorized deviation is indicated by the addition of

“(DEVIATION)” provision with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

(End of provision)

L.3 PAYMENT OF PROPOSAL COSTS

This solicitation does not commit the government to pay any cost incurred in the submission of a proposal or in making necessary studies or designs for the preparation thereof, nor to contract for services or supplies.

L.4 GENERAL PROPOSAL SUBMISSION INSTRUCTIONS AND CONDITIONS

The provision at FAR 52.212-1 (Aug 2025) (DEVIATION 25-21), Instructions to Offerors-Commercial Products and Commercial Services, applies to this acquisition and this entire document represents the addenda to the provision. This is a 100% Small Business set-aside.

The proposal must be sufficiently detailed and complete to demonstrate an understanding of an ability to comply with the requirements of this solicitation. The proposal shall demonstrate such understanding and ability in a concise, logical manner, and should not contain superfluous material that is not related directly to this acquisition. General statements that the contractor “can comply” or “will comply” with the requirements, that “standard procedures will be used,” “well known techniques will be used,” or that paraphrase the PWS in whole or part may not constitute compliance with the requirements concerning the content of the proposal volumes. Offerors must demonstrate capability of performing the required services, providing contract deliverables, outlined in this solicitation, including the PWS and all attachments, and must include convincing rationale and substantiation of all claims. Offerors shall assume the government has no prior knowledge of an offeror’s experience, ability, approaches, etc. and the government will base its evaluation on the information presented in the offeror’s proposal unless otherwise noted in this RFP.

Each proposal shall: (1) be specific and complete in every detail; (2) conform to all solicitation provisions, clauses, or other requirements; (3) be logically assembled, practical, legible, clear, concise, coherent; and indexed (cross-indexed, where appropriate); and (4) contain appropriately numbered pages of each volume or part.

The offeror’s proposal and all elements therein may be incorporated into the contract upon award. The offeror will be expected to provide the elements proposed and evidence of any tools, programs, data, software or any other such instrument submitted in the proposal as operational upon award or within any implementation timelines stated.

The government intends to evaluate and award without discussions. Therefore, the initial submission should include the most favorable terms the offeror can submit to the government for all evaluation factors. However, the government reserves the right to conduct discussions if later determined by the CO to be necessary. Additionally, the government reserves the right to establish a competitive range, and request Final Proposal Revisions for all Volumes from offerors if

determined to be necessary by the CO.

All responsible sources may submit a proposal which will be considered by the agency. However, failure to meet any requirement described anywhere in this RFP may result in rejection of the entire proposal submission, i.e. the proposal will not be accepted, evaluated, or considered for award. Further, any proposal that fails to meet every requirement cited in this RFP may be considered incomplete. If the government is unable to verify that the offeror's submission has met all RFP requirements, the entire proposal submission may be considered incomplete and the proposal may be rejected, i.e. the proposal will not be accepted, evaluated, or considered for award.

Additionally, the offeror must have an active System for Award Management (SAM) registration and must be a Small Business for the NAICS cited in this RFP at the time of proposal submission in order for the offer to be accepted. If an offeror does not have an active SAM registration or is not a Small Business for the NAICS cited in this RFP at the time of proposal submission, the entire proposal submission will be rejected in accordance with FAR 52.204-7, System for Award Management, i.e. the proposal will not be accepted, evaluated, or considered for award.

Offerors shall fully understand and accept these terms, as well as all other terms, conditions, requirements, etc. stated in the solicitation before deciding whether to participate in this RFP. Lastly, all documentation should be marked proprietary as appropriate.

L.5 COMMUNICATIONS AND POINT(S) OF CONTACT

Offerors requesting information regarding this solicitation shall contact the CO at Genna.Braden@ice.dhs.gov, only. Contacts to other government personnel or non-government advisors are prohibited. The CO or their designated representatives are the only persons authorized to contact offerors, and the CO is the only person authorized to release information regarding the ongoing procurement.

The "Subject" line of ALL correspondence shall at a minimum include "[Insert offeror name] solicitation number".

L.6 QUESTIONS

The submission deadline for questions or requests for clarifications relating to this RFP is **June 22, 2026 by 12:00 PM Central Time (CT)**. Offerors shall submit their questions, utilizing Attachment 4 – Question Template without deviation, electronically to all POC(s) listed in the Communications and Points of Contact section of this RFP via the email address(es) cited therein. No other methods of submission will be accepted. Questions or requests for clarification submitted without using Attachment 4 may not be considered at the discretion of the government. Questions or requests for clarification received after the submission deadline may be responded to at the discretion of the CO. Be advised that the government reserves the right and intends to transmit those questions and answers of common interest to all prospective offerors. As such, offerors shall

refrain from including proprietary information in their questions. Please note, the government may not provide a response to every question received. Lastly, the government will not address questions for unrelated efforts, ICE operations, nor items which are irrelevant to this RFP.

L.7 PROPOSAL SUBMISSIONS

All proposal submissions shall be provided electronically to all POC(s) listed in the Communications and Point(s) of Contact section of this RFP via the email address(es) cited therein. All submissions and volumes shall be submitted in electronic format only with file names that are consistent with the structure of the proposal. Emails shall not exceed 20 MB (megabytes) each. All email proposal submissions must be clearly marked: "70CDCR26R00000016 Proposal – [Offeror Name]" in the subject line of the email(s).

Receipt of the complete proposal package will be governed by FAR 15.107 (DEVIATION 26-08) and FAR 52.212-1 (Aug 2025) (DEVIATION 25-21). Proposals submitted by any other means not described in this solicitation will not be accepted, evaluated, or considered for award. All required proposal volumes, including modifications, must be received by the POC(s) via the email address(es) cited in the Communications and Points of Contact section of this RFP by the date and time cited in the Proposal Submission Due Date section of this RFP. The CO has determined that accepting late proposals will unduly delay the acquisition. Therefore, late proposal submissions received after the time and date cited in the Proposal Submission Due Date section of this RFP, or to the incorrect email addresses, will not be accepted, evaluated, or considered for award.

ICE shall not be responsible for late or non-delivery of offerors' proposals due to IT problems, server, or other technical issues. As such, to ensure timely receipt of proposals, offerors should NOT wait until the last moment to electronically submit proposals. It is strongly recommended that offerors request confirmation of receipt on any proposal submissions to ensure timely receipt by ICE. Offerors who require an email notification of receipt of the proposal shall provide this request prior to closing time to ensure the government is able to receive the proposal timely and provide response.

L.8 PROPOSAL SUBMISSION DUE DATE

Submissions shall be provided electronically to all POC(s) listed in the Communications and Points of Contact section of this RFP via the email address(es) cited therein by **12:00 pm CT, July 21~~7~~, 2026.** All proposal volumes must be received by the above deadline.

L.9 PROPOSAL FORMATTING

The government has not specified detailed formatting requirements for the offeror's written submissions (such as minimum margins, font size, and so forth), but expects thoughtful and purposeful engagement and professionalism focused on meeting the government's needs for the acquisition. Unnecessarily elaborate submissions beyond what is sufficient to present a complete

and effective proposal in response to this solicitation are not desired and will not instill confidence in the government evaluators. Written submissions should contain enough detail to give the government confidence that the offeror understands the requirement and can successfully complete the work. In addition, proposals which utilize illegible fonts may not be evaluated.

L.10 REQUIRED PROPOSAL VOLUMES, ORGANIZATION, AND PAGE LIMITATIONS

Offerors must submit their proposal in separate stand-alone volumes as described in the table below. Each volume shall include all required information as outlined in each respective Volume Proposal Contents and Instructions section of this RFP. Required information for each volume, which is not found in its designated volume, will be assumed to have been omitted from the proposal.

VOLUME	VOLUME TITLE	PAGE LIMITATIONS
Volume I	Proposal Summary	None
Volume II	Factor 1 – Product Offering	8
Volume III	Factor 3 – Technical Capability	10
Volume IV	Factor 3 – Past Performance and Experience	16
Volume V	Factor 4 – Price	None

Proposal contents that exceed the page limitations stated in the table above will be removed from the proposal by the CO prior to turning the proposal over to the government evaluation team, and the excess pages will not be considered or evaluated. The page limitations do not include any "front matter" information such as a title page, table of contents, table of figures, definitions, or acronyms. Any information submitted within the "front matter" will not be considered or evaluated. Note, executive summaries DO count towards the page limitations.

Pricing data and pricing assumptions shall only be included in the price volume. Pricing data is prohibited in, and shall be omitted from all other volumes. Any conditional assumptions taken with respect to the requirements and the RFP shall be fully explained in Volume I of the proposal, with the exception of any pricing assumptions. All pricing assumptions shall be explained in the pricing volume.

L.11 PROPOSAL CONTENTS AND INSTRUCTIONS: VOLUME I PROPOSAL SUMMARY

Method: Written

Required Information:

- Legal Offer: The offeror shall include a cover letter that identifies all enclosures being transmitted as part of the proposal and acknowledge that it transmits an offer in response

to the solicitation.

- RFP Number & Title
- Joint Venture (JV) and Contractor Team Arrangements (CTAs): If an offeror plans on entering into a JV or a CTA to perform the services required in this solicitation, then the offeror shall provide a copy of the JV or CTA document(s) which outlines the structure and arrangement of the JV or CTA.
- Name and address of prime, JV, CTA, and proposed subcontractors.
- Unique Entity Identifier (UEI) Number and CAGE Code
- Documentation verifying that the prime, JV, or CTA has an active SAM registration.
- Evidence the prime, JV, or CTA is currently a Small Business for the NAICS code cited in this RFP.
- Name, title, contact information, and signature of authorized representative.
- The validity period of the proposal – offerors should indicate in writing that their proposals, are valid through 9/30/2026.
- Signed SF 1449 and SF30s (if appliable): Blocks 12, 17, 23, 24, and 30 on page 1 of SF 1449 shall be completed by offerors and Block 30 shall be signed to show that the offeror has read and agrees to comply with all the conditions and instructions provided in the solicitation and all amendments. Note all applicable blocks in solicitation amendments must be addressed and the SF shall be signed by offerors.
- All assumptions must be identified in Volume I with the exception of any pricing assumptions which shall be outlined in the pricing volume.
- All required contractor provision fill-ins.

L.12 PROPOSAL CONTENTS AND INSTRUCTIONS: VOLUME II PRODUCT OFFERING

Method: Written

Required Information:

Offerors shall address ALL the below items. The government reserves the right to verify all information by any number of methods at its discretion which may be considered in the evaluation.

1. The offeror's Cloud Service Provider (CSP) must currently be Federal Risk and Authorization Management Program (FedRAMP) Authorized. Offerors must provide the full name and UEI of their CSP. The offeror shall also submit evidence from the FedRAMP Marketplace - Products website, such as a screen shot from the site, that confirms the CSP is currently FedRAMP authorized. In-Process and Ready FedRAMP Authorization statuses are not acceptable.
2. The offeror's Cloud Service Offering (CSO), such as a particular Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS) solution,

must be currently FedRAMP Authorized. Offerors must provide the full name of the CSO. The offeror shall also submit evidence from the FedRAMP Marketplace - Products website, such as a screen shot from the site, that confirms the CSO is currently FedRAMP authorized. Note, even if the CSP is FedRAMP Authorized, each individual product or service must also be FedRAMP authorized. In-Process and Ready FedRAMP Authorization statuses are not acceptable.

3. All data transmissions must be encrypted using Federal Information Processing Standard Publication (FIPS) 140-2 validated modules or National Security Agency (NSA) Type 1/2 encryption. Offerors shall confirm their solution will meet this data transmission requirement and shall provide discussion and/or evidence to support such.
4. The offeror must have the ability to provide both permanent (stationary) and mobile (portable) digital X-ray equipment and services as required, including during transition periods and for ongoing operational needs. Offerors shall confirm they have the ability to provide both permanent and portable digital X-ray equipment inclusive of services and provide discussion and/or evidence to support such.
5. The proposed solution must have the ability to integrate with government Picture Archiving and Communication System (PACS) and Electronic Health Record (eHR) systems, such as Medicor Imaging Picture Archiving and Communication System (MiPACS), and not require the government to use any proprietary PACS for image viewing. Offerors shall describe their proposed solution, confirm it meets the above requirements, and provide discussion and/or evidence to support such.
6. The proposed digital X-ray equipment and associated IT systems must support continuous monitoring, including vulnerability management, asset management, Security Information Event Management (SIEM) integration, and log retention, in compliance with FedRAMP and DHS requirements. Offerors shall describe their proposed equipment, confirm it meets the above requirements, and provide discussion and/or evidence to support such.
7. The proposed digital X-ray equipment imaging plate must meet all of the following specifications:
    a. Minimum size of 35×43 cm
    b. Maximum pixel pitch of 200 µm
    c. Matrix size of at least 3.75 megapixels
    d. Minimum 10-bit depth
    e. Spatial resolution of at least 2.5 line pairs per mm (both vertical and horizontal)
    f. Conformity with current professional standards for signal-to-noise ratio and detective quantum efficiency

    Offerors shall describe their proposed equipment, confirm it meets the above requirements, and provide discussion and/or evidence to support such.
8. The proposed equipment must have the ability to produce chest X-rays with a source-to-detector distance of at least 70 inches (180 cm). Offerors shall describe their proposed equipment, confirm it meets the above requirements, and provide discussion and/or evidence to support such.

L.13 PROPOSAL CONTENTS AND INSTRUCTIONS: VOLUME III TECHNICAL CAPABILITY

Method: Written

Required Information:

The offeror's Technical Capability must present sufficient information to reflect the offeror has a thorough understanding of the PWS requirements as well as a sound approach to successfully perform. The Technical Capability submission shall specifically address and include discussion for all the following:

- **Technical Approach**

  The offeror shall describe their understanding of the effort as well as their ability and approach to meet all requirements outlined in the PWS. Note, if the offeror's submission will be unable to meet all PWS requirements, the offeror shall explicitly outline the specific PWS requirements which their solution will be unable to meet. Additionally, the government encourages innovative approaches for achieving efficiencies provided the approach is fully explained, and appropriate risks are considered and mitigated. If proposing to exceed or add any performance requirements or standards listed in the PWS, the offeror shall clearly identify the language to include in the resulting contract. This language may be included in the contract at the discretion of the government.

- **Management and Staffing Plan**

  The offeror shall outline their management and staffing plan which discusses all the below.

  - ***Organizational Structure:*** Description of management hierarchy, subcontractor support, roles, and responsibilities for contract performance.
  - ***Staffing Plan:*** Offeror's proposed labor categories, labor mix, labor hours per category, and rationale for such. Note: Key Personnel resumes will be requested after award. ICE is not evaluating Key Personnel resumes as part of this RFP. ICE intends to evaluate and approve Key Personnel as part of contract administration.
  - ***Staffing Approach:*** Strategies for recruiting, pre-screening, and retaining qualified personnel, including compliance with ICE background investigation requirements and plans for maintaining reserve or mobile units for temporary or emergency needs.
  - ***Quality Control:*** Methods for monitoring and ensuring quality performance, including oversight of subcontractors if applicable.
  - ***Communication and Coordination:*** Processes for internal and external communication, including coordination with government stakeholders.

- **Transition-In Plan**

Offerors shall outline their Transition-In Plan which must illustrate how the offeror will achieve full operational performance within 120 day transition period. The plan must include discussion for all the below:

  - Completion of all ramp-up activities and readiness for full operational use.
  - Obtaining necessary licenses, permits, and insurance prior to performance.
  - Ensuring all employees are cleared through the required background investigation process.
  - A visual implementation schedule (e.g., Gantt chart) covering equipment ordering, delivery, installation, testing, certification, staffing, transition of government data, medical screening, training, standard operating procedures (SOPs) development, risk elements, etc.
  - Scheduling certification and training of contractor personnel to assume operational responsibilities at contract start.
  - Identification of phase-in risk areas and recommended mitigation strategies.
  - Plans for maintaining reserve or mobile units for temporary or emergency needs.

L.14 PROPOSAL CONTENTS AND INSTRUCTIONS: VOLUME IV PAST PERFORMANCE AND EXPERIENCE

Method: Written

Required Information:

Offerors shall utilize Attachment 2 – Past Performance and Experience Form and follow all instructions therein without deviation for submission of their Past Performance and Experience proposal. Utilizing Attachment 2, offerors shall provide past performance and experience information for up to four recent, relevant, and valid contract references with federal, state, or commercial organizations in which they served as the prime contractor or subcontractor for services.

See definitions below.

- Recent: Work performed within the last five years from the date of issuance of this RFP.

- Relevant: Similar in scope and magnitude to the PWS requirements.

- Valid Contract: For the purposes of this RFP, any contract not captured by the definitions below such as, but not limited to, Indefinite Delivery Indefinite Quantity (IDIQ) contracts, Blanket Purchase Agreements (BPAs), or any other parent contract are not considered valid contract references as there is no

performance at the IDIQ, BPA, or parent contract level. As such, for the purpose of defining valid contract references, a contract is defined as:

a. a Task Order (TO) or Delivery Order (DO) placed under a single-award or multiple-award contract as defined in FAR 2.101; or,
b. a single work directive or similar instrument which contains a separate Statement of Work (SOW), PWS, etc. issued under a broader contract; or,
c. a single order placed under a basic ordering agreement (BOA) FAR 16.703 (DEVIATION 26-04); or,
d. a single TO or DO placed under a federal supply schedule (FSS) FAR 8.4 (DEVIATION 25-20); or,
e. a single Blanket Purchase Agreement (BPA) Call placed under a single-award or multiple-award BPA FAR 8.4 (DEVIATION 25-20) and FAR 12 (DEVIATION 25-21); or,
f. a single government or commercial contract wherein performance was rendered which does not include any of the types of instruments described in (a)-(e) above.

At least one of the contract references submitted must be for work performed by the prime contractor as defined in FAR 3.502-1 (DEVIATION 25-35), JV as defined in FAR 2.101, or CTA partner as defined in FAR Companion (FC) 9.000. The other contract reference submissions may be from proposed subcontractor(s).

Offeror's may also submit past performance and experience information for predecessor companies. Offerors must explain the difference between the primary offering entity and the predecessor company when submitting past performance and experience information for predecessor companies. Note, past performance and experience information submitted for predecessor companies counts toward the four contract limitations and is not considered work performed by the prime, JV, or CTA as defined above.

Offerors shall also submit past performance and experience information for any subcontractor that will perform major or critical aspects of the requirements. A maximum of one valid, recent and relevant contract with federal, state, or commercial organizations for a subcontractor performing major or critical aspects of the requirements must be submitted. Note, past performance and experience information submitted for a subcontractor counts toward the four contract reference limitation.

The offeror's submission shall also include clear, concise, and complete responses to all Experience Discussion Items in Attachment 2. The offeror shall map their responses to the submitted contract references. The offeror may not use examples to answer the Experience Discussion Items from contract references other than the submitted contract references.

Past performance and experience are a measure of how well offerors and subcontractors have satisfied customers, adhered to applicable federal, state, and local laws and regulations, and conducted business in an ethical manner as well as the depth and breadth of an offeror's

experience. Offerors and subcontractors may provide information on problems encountered on the identified contracts, and the offeror's corrective actions. It is not sufficient to merely state that past or ongoing contracts are valid, recent, and relevant to the requirements of the PWS. Rationale shall be provided to convincingly demonstrate that such contracts are indeed recent, relevant, and valid. The offeror is responsible for verifying and ensuring that the information provided in support of its cited past performance and experience is complete, comprehensive, accurate, and current as of the date of submission. The government will neither make assumptions nor draw inferences regarding missing or incomplete information. Offerors are reminded of the penalties for making false statements prescribed by 18 U.S.C. 1001.

Offerors are advised that past performance and experience information may be obtained from other sources known to the government, and therefore, the government may also evaluate information from such other sources, even though the offeror does not include such information in its proposal. The overall past performance and experience rating determined will be based upon the past performance and experience information received for both the offeror and subcontractor(s) and any other information obtained by the government.

L.15 PROPOSAL CONTENTS AND INSTRUCTIONS: VOLUME V PRICE

Method: Written

Required Information:

Offerors shall use Attachment 3 - Pricing Template without deviation and follow all instructions therein for submission of their Price proposal. The offeror shall not hide any cost cells and provide viewable formula access to all cells. All items covered under option years may be ordered and performed during the scheduled period of performance of this contract. As such, offerors are required to provide prices for all items under option periods. Proposed pricing shall be inclusive of all costs associated with the effort such maintenance costs, warranty, etc. as applicable. Additionally, proposed transition pricing shall be inclusive of all costs to procure, deliver, install, inspect, and certify equipment for use. Note, quantities cited in Attachment 3 are estimates only and are not to be misconstrued as a minimum or maximum amount. Lastly, as part of the pricing volume offerors may also submit a written narrative.

[END OF SECTION L]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

SECTION M - EVALUATION FACTORS FOR AWARD

M.1 FAR PROVISIONS INCORPORATED BY REFERENCE

In accordance with (IAW) FAR 52.252-1, the following clauses are incorporated by reference:

Number	Title	Date
52.217-5	Evaluation of Options (DEVIATION 25-36)	Sep 2025

M.2 GENERAL

An offeror which takes exception to government terms or proposes additional or alternate terms, runs the risk that the government may find the offer is nonconforming and/or unacceptable. The proposals shall be submitted in accordance with the requirements in this RFP. An offer may be rejected as deficient if the CO determines that the proposal does not comply with the RFP requirements.

The government may:

- Reject the entire proposal if such action is in the public interest;
- Reject the entire proposal if the CO determines any aspect of the offer does not comply with the RFP instructions or any other RFP requirement, term, etc.
- Accept other than the lowest price proposal; and/or
- Waive informalities and minor irregularities as determined by the government in proposals received.

M.3 BEST VALUE AND AWARD DECISION

The government anticipates awarding a FFP single award IDIQ contract to the responsible offeror whose proposal conforms to the solicitation and will be most advantageous to the government, price and other factors considered. The government may award to other than the lowest priced offeror, or other than the offeror with the highest non-price rating.

The best value trade off approach, which will be utilized for this acquisition, is a method of selecting the proposals that represents the best value to the government, based on the evaluation of each proposal. The government evaluation team will present its findings to the Source Selection Authority (SSA). The SSA's award decision shall be based on a comparative assessment of proposals against all source selection criteria in the solicitation. While the SSA may use reports and analyses prepared by others, the award decision shall represent the SSA's independent judgment.

The government will evaluate proposals in accordance with the requirements of FAR 15.2 *"Evaluation and Award"* (DEVIATION 26-08). Offerors must recognize that the initial evaluation of proposals and the determination of the competitive range, as applicable, will be made upon a review of the proposals only, plus some government independent investigations as previously outlined. The government may seek revised proposals from offerors within the

competitive range.

At the conclusion of discussions, if applicable, FAR 15.204-2(d)(DEVIATION 26-08), will be followed for any proposal revision. The final proposal revision (FPR) shall be submitted in the form of a contractual document (including revisions to the original proposal) that has been executed by an individual with the authority to bind the offeror. Selection will be made in accordance with the evaluation criteria herein. Contract award may be made without subsequent discussions or negotiations.

M.4 EVALUATION FACTORS

Offeror's will be evaluated based on the following non-price factors and price.

Factor 1 – Product Offering (go/no go factor)
Factor 2 – Technical Capability (non-price trade-off factor)
Factor 3 – Past Performance and Experience (non-price trade-off factor)
Factor 4 – Price (trade-off factor)

M.5 EVALUATION FACTOR ORDER OF IMPORTANCE

As noted in the Evaluation Process section of this RFP, Factor 1: Product Offering will be evaluated first on a go/no-go ("Acceptable/Unacceptable") basis. While Factor 1: Product Offering will be considered in the overall best value award determination, it is not a trade-off factor. The trade-off evaluation factors are listed below in descending order of importance.

- Technical Capability (non-price trade-off factor)
- Past Performance and Experience (non-price trade-off factor)
- Price (trade-off factor)

The non-price trade-off factors, Technical Capability and Past Performance and Experience, are more important than the Price factor. If the non-price factor evaluation of proposals determines there are no substantial differences between the proposals, then price becomes more important, but not necessarily determinative, in making the award decision. Note, award may be made to other than the offeror with the lowest priced offer, if the government determines that a price premium is warranted due to technical merit. The government may also award to other than the highest technically rated offer, if the government determines that a price premium is not warranted.

M.6 EVALUATION PROCESS

The government will employ a two-step evaluation process. Factor 1: Product Offering will be evaluated first on a go/no-go ("Acceptable/Unacceptable") basis. Offerors whose submissions are rated Unacceptable for Factor 1: Product Offering will be ineligible for award, will be eliminated from the competition, and their trade-off factor proposals, (Technical Capability, Past Performance and Experience, and Price) will not be evaluated.

Offerors whose submissions are rated “Acceptable” for Factor 1: Product Offering will have their trade-off factor proposals evaluated.

M.7 EVALUATION PROCESS: PRODUCT OFFERING

Factor 1: Product Offering will be evaluated first on a go/no-go (“Acceptable/Unacceptable”) basis. The offeror’s Product Offering submission will be evaluated to determine whether the proposal meets ALL the below criteria:

1. The offeror’s CSP is currently FedRAMP Authorized. In-Process and Ready FedRAMP Authorization statuses are not acceptable.

2. The offeror’s CSO, such as a particular SaaS, PaaS, or IaaS solution, is currently FedRAMP Authorized. In-Process and Ready FedRAMP Authorization statuses are not acceptable.

3. All data transmissions are encrypted using FIPS 140-2 validated modules or NSA Type 1/2 encryption.

4. The offeror can provide both permanent (stationary) and mobile (portable) digital X-ray equipment and services as required, including during transition periods and for ongoing operational needs.

5. The proposed solution has the ability to integrate with government PACS and eHR systems, such as MiPACS, and does not require the government to use any proprietary PACS for image viewing.

6. The proposed digital X-ray equipment and associated IT systems support continuous monitoring, including vulnerability management, asset management, SIEM integration, and log retention, in compliance with FedRAMP and DHS requirements.

7. The proposed digital X-ray equipment imaging plate meets all of the following specifications:

    a. Minimum size of 35×43 cm
    b. Maximum pixel pitch of 200 μm
    c. Matrix size of at least 3.75 megapixels
    d. Minimum 10-bit depth
    e. Spatial resolution of at least 2.5 line pairs per mm (both vertical and horizontal)
    f. Conformity with current professional standards for signal-to-noise ratio and detective quantum efficiency

8. The proposed equipment has the ability to produce chest X-rays with a source-to-detector distance of at least 70 inches (180 cm).

The Factor 1: Product Offering proposal will be rated acceptable or unacceptable, based on the rating definitions in the table below.

Rating Definitions	
Acceptable	The proposal meets ALL of the above criteria.
Unacceptable	The proposals fails to meet one or more of the above criteria.

M.8 GENERAL EVALUATION PROCESS NON-PRICE TRADE-OFF FACTORS

The government will evaluate and assess its level of confidence that the offeror will be successful in performing the requirements based on an analysis of the offeror's Factor 2 and Factor 3 submissions. The government will evaluate the proposals and document its evaluation through Confidence Findings as defined in the table below for each of the non-price trade-off factor proposals.

Confidence Findings Definitions	
Element that Increases Confidence	An aspect/element in the proposal that has an appreciable positive impact on the government's confidence.
Element that Decreases Confidence	An aspect/element in the proposal that poses a risk of unsuccessful contract performance and has an appreciable negative impact on the government's confidence.
Deficiency	A material failure of a proposal to meet a government requirement or a combination of elements in a proposal that increases the risk of unsuccessful contract performance to an unacceptable level. A Deficiency finding may result in a rating of Low Confidence for the submission.
Observation	An aspect/element which the government wishes to highlight that does not have a positive or negative impact on the government's evaluation.

M.9 EVALUATION PROCESS: TECHNICAL CAPABILITY

The government will evaluate and assess its level of confidence that the offeror understands the PWS requirements, has sound approaches, and will be successful in performing based on the offeror's Technical Capability submission. Note, submissions which simply offer to perform in accordance with the government's requirements, merely paraphrase the requirements document, or use simple statements of compliance or reiteration (e.g. "understood", "will comply", "has the capability to", "well-known techniques will be used", etc.) may not provide confidence to the government evaluators. The government will evaluate the Technical Capability submission and will document its evaluation through Confidence Findings as defined in the General Evaluation Process Non-Price Trade-Off Factor section of this RFP. An offeror's Technical Capability submission will be evaluated as outlined above and assigned a Confidence Rating as described in the table below.

Confidence Rating Definitions	
High Confidence	The government has high confidence that the offeror understands the requirement, proposes a sound approach, and will be successful in performing/managing the contract with little to no government intervention.
Some Confidence	The government has some confidence that the offeror understands the requirement, proposes a sound approach, and will be successful in performing/managing the contract with some government intervention.
Low Confidence	The government has low confidence that the offeror understands the requirement, has proposed sound approaches, will be successful in performing/managing the contract requirements even with government intervention.

M.10 EVALUATION PROCESS: PAST PERFORMANCE AND EXPERIENCE

The government will evaluate and assess its level of confidence that the offeror will be successful in performing the requirements based on an analysis of the offeror's Past Performance and Experience submission. The government may also evaluate past performance and experience information obtained through customer Past Performance Questionnaires (if applicable), Contractor Performance Assessment Reporting System (CPARS), similar systems of other government departments and agencies, interviews, and through any other sources known to the government, including commercial sources. While the government may elect to consider data obtained from other sources, the burden of providing current, accurate and complete past performance and experience information rests with the offeror.

In the case of an offeror without a record of recent and relevant past performance or for whom information on past performance is not available or so sparse that no meaningful past performance rating can be reasonably assigned, the offeror may not be evaluated favorably or unfavorably on past performance 15.202(c)(1) (DEVIATION 26-08). Therefore, the offeror shall be determined to have "Unknown Confidence" or neutral past performance.

The government will evaluate the Past Performance and Experience submission, along with any other information obtained by the government, and will document its evaluation through Confidence Findings as defined in the General Evaluation Process Non-Price Trade-Off Factor section of this RFP. An offeror's Past Performance and Experience will be evaluated as outlined above and assigned a Confidence Rating as described in the table below.

Contract Rating Definitions	
High Confidence	Based on the offeror's Past Performance and Experience, the government has high confidence that the offeror will be successful in performing the contract requirements with little to no government intervention.
Some Confidence	Based on the offeror's Past Performance and Experience, the government has some confidence that the offeror will be successful in performing the contract requirements with some government intervention.
Low Confidence	Based on the offeror's Past Performance and Experience, the government has low confidence that the offeror will be successful in performing the contract requirements even with government intervention.
Unknown Confidence (Neutral)	The offeror does not have recent and relevant past performance, or any performance record. Or, the offeror's past performance is so sparse, a meaningful confidence rating cannot be reasonably assigned.

M.11 EVALUATION PROCESS: PRICE

Price proposals will not be assigned a confidence rating but will be evaluated with respect to completeness and reasonableness based on the information submitted in the offeror's price submission. As part of the price evaluation, the government will evaluate the extension period authorized by FAR 52.217-8, "Option to Extend Services." The pricing for evaluation of FAR 52.217-8 will be derived by dividing the total amount of Option Period 4 by a factor of two. Additionally, the maximum for this IDIQ will be calculated based on the total proposed value of the base and all option periods multiplied by a factor of 115%. This amount will be stated in the IDIQ award as a dollar amount. Thus, for the purposes of evaluation under this RFP, the offeror's total evaluated price will include the base period, all option periods, and the FAR 52.217-8 Option to Extend Services pricing with the 115% factor applied to all items. Note, a separate Contract Line Item Number (CLIN) will not be included in the contract for the FAR 52.217-8 pricing.

The Price proposal may also be compared to the offeror's proposal volumes for consistency. Price Proposal evaluations may include an analysis for unbalanced pricing as referenced in FAR 15.404-6 (DEVIATION 26-08). A determination of unbalanced pricing may lead to the rejection of the entire offer, i.e. the offeror will not be considered for award as permitted in FAR 15.404-6(b)(2) (DEVIATION 26-08).

Completeness. The government's price evaluation will assess the completeness of the price proposal, which involves verification of all the below. If the government is unable to verify if the offeror has completed all the below items, the price proposal may be considered incomplete, which may affect the government's ability to determine whether the proposed price is reasonable.

- All line items in Attachment 3 – Pricing Template are priced.

- All figures are correctly calculated, and no formulas are hidden.

Reasonableness. The government will evaluate the total proposed price for reasonableness. The government may utilize one or more of the techniques specified in FAR 15.404-1 (DEVIATION 26-08).

[END OF SECTION M]

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]