SECTION II – STATEMENT OF WORK

1 BACKGROUND

The U.S. Department of Homeland Security (DHS), Office for Civil Rights and Civil Liberties (CRCL), is responsible for investigating complaints filed pursuant to 6 U.S.C. § 345 and 42 U.S.C. § 2000-ee-1, alleging abuses of civil rights, civil liberties, and racial and ethnic profiling by DHS employees and officials, as well as contractors used by DHS Components. CRCL's Compliance Branch is responsible for investigating these complaints. CRCL is also charged with overseeing compliance with constitutional, statutory, regulatory, policy, and other requirements relating to the civil rights and civil liberties of individuals affected by DHS programs and activities.

2 SCOPE

2.1 The purpose of this contract is to obtain Medical Doctor SME Services to assist CRCL in performing its investigatory and oversight functions. The selected subject matter expert shall primarily assist CRCL in conducting investigations involving medical issues in immigration detention facilities used by U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP), which shall include preparing reports related to the investigations. CRCL cannot accurately predict the locations nor the number of facilities that may require onsite reviews because it depends on the complaints received. The expert may also be asked to assist CRCL with other CRCL matters related to medical care, including reviews initiated by DHS leadership, consulting with substantive work groups, providing training, and other activities as requested.

2.2 Medical Doctor SME services are required to evaluate complaints received pursuant to 6 U.S.C. § 345 and 42 U.S.C. § 2000-ee-1 and to oversee compliance with constitutional, statutory, regulatory, policy, and other requirements related to civil rights and civil liberties. In addition to evaluating complaints, the contractor shall provide assistance related to activities that arise within CRCL's authority, including, but not limited to research, analysis, and/or development of system-wide standards, policies, procedures, and training. Services include, but are not limited to, conducting reviews of DHS facilities, providing training related to their areas of expertise, and other activities and projects related to medical care concerns, as tasked by CRCL, such as participating in work groups, developing, or presenting briefings, and preparation of documents. In particular, the experts shall also be required to prepare detailed reports regarding their observations and findings, as well as to provide recommendations based upon applicable correctional standards. CRCL cannot accurately predict the extent of the related activities required because it depends on the complaints received.

3 REQUIREMENTS/TASKS

3.1 The Contractor shall review, evaluate, and report on medical issues and advise CRCL on how Department policies and practices impact various issues involving immigration detention facilities.

3.2 The Contractor personnel shall document their findings and recommendations in well written, comprehensive reports for each investigation or assignment. The Contractor personnel shall collaborate with CRCL as necessary to make edits to the written reports in order to fulfill CRCL's needs, goals, and requirements.

3.3 The Contractor personnel shall provide CRCL with guidance on various violations of civil rights or

civil liberties related to medical practices upon request, whether related to a CRCL investigation, or related to a broader CRCL issue or area of work. The Contractor personnel shall provide such guidance, whether planned or ad hoc, by telephone, email, formal report, or in person, as requested by CRCL. The guidance shall include, but not be limited to, discussions and assessments of individual cases, findings from onsite investigations, discussion of policies and practices, and any other relevant information that may arise during the course of an investigation or other aspects of CRCL's oversight work.

4 CONTRACTOR PERSONNEL

4.1 QUALIFIED PERSONNEL

The Contractor shall provide qualified Medical Doctor consultants to perform the requirements specified in this Statement of Work.

4.2 MINIMUM REQUIREMENTS FOR A MEDICAL DOCTOR CONSULTANT SUBJECT MATTER EXPERT

4.2.1 The Contractor shall maintain an active medical license in at least one state and be board certified in family medicine or internal medicine.

4.2.2 The Contractor shall have at least 10 years of experience providing medical care in an adult detention setting.

4.2.3 The Contractor has certifications or special training related to providing medical care in a correctional setting, such as Certified Correctional Health Professional.

4.2.4 The Contractor shall be experienced investigating, auditing, or otherwise evaluating detention facilities for adherence to applicable standards related to medical care programs and systems.

4.2.5 The Contractor shall have experience objectively critiquing the treatment provided by other medical practitioners in a detention setting.

4.2.6 The Contractor shall have experience serving as a subject matter expert providing advice, guidance, or testimony on the operation of medical care programs or systems in a detention setting.

4.2.7 The Contractor shall have experience formulating recommendations or other steps to address issues, violations, or concerns identified as part of an investigation or other type of inquiry.

4.2.8 The Contractor shall have experience applying the American Correctional Association (ACA) Standards, National Commission on Correctional Health Care (NCCHC) Standards, and other standards related to medical care in a detention setting.

4.2.9 The Contractor shall have knowledge and experience with the history, policies, and protocols of medical care in a detention setting and will be apprised of recent trends and developments in providing these services.

4.2.10 The Contractor shall have experience producing written reports that evaluate detention standards, systems, and actions present in detention facilities. This will include analysis of and application of

standards and policy.

4.2.11 The Contractor shall demonstrate the ability to produce comprehensive reports that are well-written, clear, and cite relevant resources.

4.2.12 The Contractor shall demonstrate the ability to review large amounts of documentary evidence in short timeframes and provide oral briefings, written reports, and training under tight timelines.

4.2.13 TRAVEL: The Contractor personnel must be able to travel to various locations nationwide (CONUS) to perform onsite investigations for several consecutive days and work efficiently and cooperatively under the direction of CRCL personnel. Travel to be paid in accordance with the Federal Travel Regulations (FTR).

4.3 Other Contractor Features, but not required

The following are contractor features above the minimum requirements of qualified personnel, but are not required for SECTION II performance:

4.3.1 The Contractor has more than the minimum requirement of 10 years of experience providing medical care in an adult detention setting.

4.3.2 The Contractor has experience managing a health care program in a detention or other setting.

4.3.3 The Contractor has demonstrated experience in a variety of types of detention settings and with a variety of populations. The variety could include working with adults and children, working in prisons, jails, or another type of facility, or working with other special populations.

4.3.4 The Contractor has provided medical care in an immigration detention facilities.

4.3.5 The Contractor has conducted and published research and analysis regarding system-wide issues related to medical health care in a detention setting.

4.3.6 The Contractor has worked directly with the ICE National Detention Standards (NDS), Performance Based National Detention Standards (PBNDS), or other related policies governing medical care in immigration detention. The Contractor has certifications or special training related to providing medical care in a correctional setting, such as Certified Correctional Health Professional.

4.3.7 The Contractor has reviewed and evaluated medical services provided in an immigration detention facility.

4.3.8 The Contractor has multiple key personnel who meet the minimum requirements in the statement of work.

SECTION III – DELIVERIES AND PERFORMANCE

1 PERIOD OF PERFORMANCE

The period of performance for work performed under this contract consists of a one-year base period of performance and four (4) one-year optional periods of performance.

Base Period	9/2024 - 9/2025
Option Period 1	9/2025 – 9/2026
Option Period 2	9/2026 – 9/2027
Option Period 3	9/2027 – 9/2028
Option Period 4	9/2028 – 9/2029

2 PLACE OF PERFORMANCE

The place of performance for work performed under this contract shall be the Contractor's site or Contractor's remote location (CONUS). The contractor shall also perform work onsite at locations to be determined by CRCL.

3 HOURS OF OPERATION

Services will generally not be required on the following Federal holidays (or any other holidays declared by the Government); however, the Contractor may be required to provide services on these days in support of mission critical situations.

- New Year's Day
- Martin Luther King's Birthday
- Inauguration Day (Metropolitan DC only)
- President's Day
- Memorial Day
- Juneteenth
- Independence Day
- Labor Day
- Columbus Day
- Veteran's Day
- Thanksgiving Day
- Christmas Day

No work shall be performed by Contractor personnel on Government facilities on Federal holidays or other non-workdays without prior written approval of the Contracting Officer Representative (COR).

4 DELIVERABLES AND DELIVERY SCHEDULE

The Government will review all draft and final deliverables to ensure accuracy, functionality, completeness, professional quality, and overall compliance with government policies, regulations, laws, and directives. Written documents shall be concise and clearly written.

Final documentation deliverables shall be provided in hard and soft copy using MS Office applications. Daily, weekly, and interim information deliverables and working-copy products may be provided by email or disk, as arranged with the COR.

The government will have ten (10) business days to accept or reject contract deliverables. If a deliverable is rejected and returned to the Contractor for revision, the Contractor shall provide the corrected deliverable within five (5) business days of notification of the request for revision.

All deliverables shall be submitted to the COR and assigned CRCL POC identified in this contract. The Contractor's deliverables shall not contain any identifiable corporate markings.

ITEM	DELIVERABLE / EVENT	DUE BY
1	**Post Award Meeting**	5 business days of date of award.
2	**Progress Reports**	3 business days following request.
2	**Draft Investigative Reports**	**COR CHECKPOINT** Within 10 business days of receipt of assignment or completion of investigative work: Contractor shall submit draft to COR and assigned CRCL POC for review. The Contractor and CRCL will discuss the draft report to ensure its accuracy. CRCL will furnish comments and edits to Contractor who shall be responsible for making changes to the draft. The COR must be copied on all assignment correspondence.
3	**Oral Briefings and Ad Hoc Reports or Project-related work**	**COR CHECKPOINT** Due date to be determined by COR and/or assigned CRCL POC and Contractor
4	**Edits to Reports and Documents**	5 business days after receipt of government comments.

4.1.1 Government Acceptance Period

The COR and assigned CRCL POC will review deliverables prior to acceptance and provide the contractor with an e-mail that conveys acceptance or documented reasons for non-acceptance. The COR or assigned CRCL POC will have ten (10) business days to review deliverables and provide notification of acceptance or rejection.

4.1.2 Post Award Meeting

The Contractor shall participate in a Post Award Meeting with the CO and the COR no later than five (5) business days after the date of award. The purpose of the Post Award Meeting is to discuss the contracting objectives of this contract. The Post Award Meeting will be held at the Government's facility or conference call.

4.1.3 Kick-Off Meeting

The Contractor shall attend a Kick-Off meeting with the COR and members of the Program Office no later than 5 business days after the date of award. The purpose of the Kick-Off meeting, which will be chaired by the COR, is to discuss the technical objectives of this contract. The Kick-Off meeting will be held at the Government's facility, located in Washington, DC or by conference call. The specifics of the meeting will be provided upon contract award.

4.1.4 Progress Reports

The Program Manager (Contractor) shall provide progress reports as needed to the COR via electronic mail. This report shall include a summary of all Contractor work performed, including an assessment of technical progress, written and analytical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

4.1.5 Government Furnished Resources

The Government will provide all necessary information, data and documents to the Contractor for work required under this task order.

The Government will provide a government furnished laptop. All electronic work product must be saved by the contractor on the DHS network drives and folders and not on the local drive.

The contractor will ensure continued connectivity to the DHS network by logging on to the DHS laptop as outlined by information technology.

SECTION IV – CONTRACT ADMINISTRATION DATA

1 POST- AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the CO and COR no later than 5 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the CO, is to discuss contracting objectives of this task order. The Post Award Conference will be held at the Government's facility, located in Washington, DC or by conference call. The specifics of the meeting will be provided upon task order award.

2 TASK ORDER KICK-OFF MEETING

The Contractor shall attend a Task Order Kick-Off meeting with the COR and members of the Program Office no later than 5 business days after the date of award. The purpose of the Task Order Kick-Off meeting, which will be chaired by the COR, is to discuss the technical objectives of this task order. The Task Order Kick-Off meeting will be held at the Government's facility, located in Washington, DC or by conference call. The specifics of the meeting will be provided upon task order award.

3 CONTRACTING OFFICER

The Contracting Officer is the only individual who can legally commit or obligate the Government for the expenditure of public funds and authorize revisions of the terms and conditions of this contract. The Contracting Officer shall authorize any such revision in writing.

The Contracting Officer is:

The Contract Specialist is:

4 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The COR for this contract is: TBD

Note: The COR's contact information will be provided at contract award.

SECTION V - INVOICE AND PAYMENT PROVISIONS

1 INVOICES

Invoices shall be prepared in accordance with FAR Clauses 52.232-25 Prompt Payment. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1. Name and address of the contractor.
2. Invoice date and invoice number. (Contractors should date invoices as close as possible to the date of mailing or transmission.)
3. Contract number and period of performance or other authorization for supplies delivered or services performed (including order number and contract line-item number).
4. Description (the associated CLIN, dollar amount invoiced, and service completed). All invoices shall include the current amount billed along with a cumulative amount billed and remaining balance.
5. Shipping and payment terms (e.g., shipment number and date of shipment, discount for prompt payment terms). Any other information or documentation required by the Contract (e.g., evidence of shipment)
6. Name and address of contractor official to whom payment is to be sent (must be the same as that in www.sam.gov).
7. Name (where practicable), title, phone number, and mailing address of person to notify in the event of a defective invoice.
8. Electronic funds transfer (EFT) banking information.
   The Contractor shall submit one invoice by the 5th day of each month.
   The Contractor shall submit the invoice electronically to the email address below:
   E-mail: [redacted]

   The Contractor shall simultaneously provide an electronic copy of the invoice to the following individuals at the email addresses below:
   A) ATTN: Office of Procurement Operations/
      E-mail
   B) ATTN: Office of Procurement Operations
      E-mail:
   C) ATTN: Office of Civil Rights and Civil Liberties /COR TBD
      E-mail: TBD

SECTION VI – SPECIAL CONTRACT REQUIREMENTS

1) CONTRACTOR PERSONNEL SECURITY CLEARANCE REQUIREMENT

All contractor and subcontractor personnel are required to complete a suitability/background investigation with the DHS Office of Security, Personnel Security Division.

The procedures outlined below shall be followed for the DHS Office of Security, Personnel Security Division (PSD) to process suitability/background investigations and suitability determinations, as required, in a timely and efficient manner.

Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

Contractor employees (to include applicants, temporaries, part-time and replacement employees) under the contract, requiring access to sensitive information, shall undergo a position-sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate suitability/background investigation to be conducted. All suitability/background investigations will be processed through the DHS Office of Security Office/PSD. Prospective Contractor employees shall submit the following completed forms to the DHS Office of Security Office/PSD. The Standard Form (SF) 85P will be completed electronically, through the Office of Personnel Management's e-QIP SYSTEM. The completed forms must be given to the DHS Office of Security Office/PSD no less than thirty (30) days before the start date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

a) Standard Form (SF) 85-P — Questionnaire for Public Trust Positions
b) SF-85P Certification
c) SF-85P Authorization for Release of Information
d) FD Form 258 — Fingerprint Card (2 copies)
e) DHS Form 11000-6 — Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement
f) DHS Form 11000-9 — Disclosure and Authorization Pertaining to Consumer Reports pursuant to the Fair Credit Reporting Act

Only complete packages will be accepted by the DHS Office of Security/PSD. Specific instructions on submission of packages will be provided upon award of the contract.

The DHS OCSO/PSD may, as it deems appropriate, authorize and grant a favorable Entry on Duty (EOD) decision based on preliminary checks. A favorable EOD decision allows a contractor employee to commence work temporarily prior to the completion of the full background investigation. The granting of a favorable EOD decision shall not be considered as assurance that a favorable fitness determination will follow. In addition, a favorable EOD or fitness determination shall in no way prevent, preclude, or bar DHS from withdrawing or terminating access to government facilities or information, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD or fitness determination by the DHS OCSO/PSD. Limited access to Government buildings is allowable without an EOD decision if the Contractor is escorted by a Government employee and the purpose of the visit is to attend a limited number of required briefings or nonrecurring meetings in order to facilitate the transition of a contract.

Medical Doctor Subject Matter

The intent of this statement is to allow a minimum amount of meetings/transition attendances to prepare for a new contract.

The DHS OCSO/PSD 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 identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have a favorable Entry on Duty or fitness determination by the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD), to access this information.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

2) SECURITY OFFICE CONTACT

Office of Security/PSD
Customer Service Support
Washington, DC 20528
Telephone: [redacted]
E-mailbox: [redacted]

3) DISCLOSURE OF INFORMATION

Information furnished under this contract may be subject to disclosure under the Freedom of Information Act (FOIA). Therefore, all items that are confidential to business, or contain trade secrets, proprietary, or personnel information must be clearly marked. Marking of items will not necessarily preclude disclosure when DHS or the Government determines disclosure is warranted by FOIA. However, if such items are not marked, all information contained within the submitted documents will be deemed to be releasable.

Any information made available to the Contractor by the Government must be used only for the purpose of carrying out the provisions of this contract and must not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract.

In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and must ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees.
Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed must be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such information, by any means, for a purpose or to an extent

unauthorized herein, may subject the offender to criminal sanctions imposed by 18 USC 641.

Notification of consulting teaching, speaking, and writing activities: Contractor employees shall notify the Contracting Officer's Representative before engaging in consulting, teaching, speaking, or writing activities if:

- The information conveyed through the activity draws substantially on knowledge or official data that are nonpublic information as defined in 5 C.F.R. § 2635.703(b);
- The subject of the activity deals in significant part with work performed under the contract; or
- The subject of the activity deals in significant part with any ongoing or announced policy, program, or operation of the agency.

Notice shall be provided at least seven days prior to engaging in the activity. The scope of the notification is not intended to include work in the expert's area of expertise that does not derive from work done for DHS.

Disclosures of Information in Litigation: Contractor employees shall comply with 6 C.F.R. Part 5, Subpart C, including 6 C.F.R. §§ 5.44 and 5.49. Those regulations generally prohibit contractor employees from testifying in connection with litigation based upon information acquired in the scope and performance of their official Department duties, except as authorized by the Department.

Notice Regarding Appearance of Conflict

The nature of the work under this contract includes circumstances where Contractor personnel will likely investigate allegations and/or complaints pertaining to law enforcement issues within DHS Components. Contractor personnel either currently providing work for a DHS Component that is the same or similar in scope to the requirement under this contract, or who have provided the same or similar work for a DHS Component in the three years prior to the start of this contract, are not eligible to perform services on this contract in order to prevent the existence or appearance of conflicting roles that might affect a contractor's judgement.

The Contractor shall not employ any person under this contract who is an employee of the United States Government if that employment would, or would appear to, cause a conflict of interest. The Contractor shall notify the Contracting Officer and Contracting Officer's Representative by telephone and in writing within 72 hours when a conflict of interest arises during the course of carrying out the duties of this contract.

4) NON-PERSONAL SERVICES

The services required under the contract constitute professional support services, which are essential to the mission but not otherwise available within. The Government will neither supervise Contractor employees nor control the method by which the Contractor performs the required tasks. Under no circumstances shall the Government assign tasks to, or prepare work schedules for, individual Contractor employees. It shall be the responsibility of the Contractor to manage their employees and to guard against any actions that have the nature of personal services or give the perception of personal services. If the Contractor feels that any actions constitute, or are perceived to constitute personal services, it shall be the Contractor's further responsibility to notify the Contracting Officer immediately.

These services shall not be used to perform work of a policy/decision making or management nature. All

decisions relative to programs supported by the Contractor will be the sole responsibility of the Government. Support services will not be ordered to circumvent personnel ceilings, pay limitations, or competitive employment procedures.

OTHER APPLICABLE CONDITIONS

5) FAR 52.224-3 Privacy Training – Alternate I (DEVIATION 17-03) (July 2023)

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

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

(1) Have access to a system of records;

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

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

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

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

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

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

(1) Have access to a system of records;

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

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

(End of clause)

INFORMATION TECHNOLOGY SECURITY AWARENESS TRAINING (JULY 2023)

(a) *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.

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that 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.

(2)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 clause)

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

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

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

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

(i) Truncated SSN (such as last 4 digits);
(ii) Date of birth (month, day, and year);
(iii) Citizenship or immigration status;
(iv) Ethnic or religious affiliation;

(v) Sexual orientation;
(vi) Criminal history;
(vii) Medical information; and
(viii) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

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

(b) *PII and SPII Notification Requirements.*

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

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

(3) Subject to government analysis of the incident and direction to the Contractor regarding any resulting notification, the notification method may consist of letters to affected individuals sent by first-class mail, electronic means, or general public notice, as approved by the Government. Notification may require the Contractor's use of address verification and/or address location services. At a minimum, the notification shall include:
(i) A brief description of the incident;
(ii) A description of the types of PII or SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, mitigate the incident, and protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

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

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

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

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts.
(3) Establish a dedicated call center. Call center services shall include:
(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;
(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;

(v) Customized Frequently Asked Questions, approved in writing by the Contracting Officer in coordination with the Component or Headquarters Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(End of clause)

HSAR 3052.204-72 Safeguarding of Controlled Unclassified Information.

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

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);
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

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

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

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

(i) Inspections;
(ii) Investigations;
(iii) Forensic reviews;
(iv) Data analyses and processing; and
(v) Revocation of the Authority to Operate (ATO), if applicable.

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

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

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

the sanitization of all government and government-activity related files and information. The Contractor shall submit the certification to the COR and Contracting Officer following the template provided in NIST SP 800–88, *Guidelines for Media Sanitization*, Appendix G.

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

(g) *Subcontracts.* The Contractor shall insert this clause in all subcontracts and require subcontractors to include this clause in all lower tier subcontracts when subcontractor employees will have access to CUI; CUI will be collected or maintained on behalf of the agency by a subcontractor; or a subcontractor information system(s) will be used to process, store, or transmit CUI.

(End of clause)

ALTERNATE I (JULY 2023)

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

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

(1) *Complete the Security Authorization process.* The Security Authorization (SA) process shall proceed according to DHS Policy Directive 4300A *Information Technology System Security Program, Sensitive Systems* (Version 13.3, 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)

SECTION VII – CONTRACT CLAUSES

1. CLAUSES INCORPORATED BY REFERENCE

Federal Acquisition Regulation (FAR) Clauses / Provisions		
Clause	**Title**	**Date**
52.203-16	Preventing Personal Conflicts of Interests	Jun 2020
52.204-9	Personal Identity Verification of Contractor Personnel	Jan 2011
52.204-14	Service Contract Reporting Requirements	Oct 2016
52.216-31	Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition	Nov 2021
52.217-5	Evaluation of Options	Jul 1990
52.222-50	Combating Trafficking in Persons	Nov 2021
52.224-3	Privacy Training Alternate 1	Jan 2017
Homeland Security Acquisition Regulation (HSAR) Clauses / Provisions		
Clause	**Title**	**Date**
3052.203-70	Instructions for Contractor Disclosure of Violations	Sep 2012
3052.205-70	Advertising, Publicizing Awards and Releases	Sep 2012
3052.228.70	Insurance	Dec 2003
3052.242-72	Contracting Officer's Technical Representative	Dec 2003
3052.204-73	Notification and Credit Monitoring Requirements for personally Identifiable Information Incidents	July 2023
3052.204-72	Safeguarding of Controlled Unclassified Information	July 2023

2 INCORPORATED BY FULL TEXT

FAR 52.204–24, REPRESENTATION REGARDING CERTAIN TELECOMMUNICATIONSAND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (NOV 2021)

The Offeror shall not complete the representation at paragraph (d)(1) of this provision if the Offeror has represented that it "does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument" in paragraph (c)(1) in the provision at 52.204-26, Covered Telecommunications Equipment or Services—Representation, or in paragraph (v)(2)(i) of the provisionat 52.212-3, Offeror Representations and Certifications-Commercial Items. The Offeror shall not complete the representation in paragraph (d)(2) of this provision if the Offeror has represented that it "does not use covered telecommunications equipment or services, or any equipment, system, or service that uses covered telecommunications equipment or services" in paragraph (c)(2) of the provision at 52.204-26, or in paragraph (v)(2)(ii) of the provision at 52.212-3.

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

Backhaul, covered telecommunications equipment or services, critical technology, interconnection arrangements, reasonable inquiry, roaming, and substantial or essential component have the meanings provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(b) *Prohibition.*

(1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system,

or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover 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) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract or extending or renewing a contract with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract. Nothing in the prohibition shall be construed to—

(i) Prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(ii) Cover 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) *Procedures.* The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered telecommunications equipment or services".

(d) *Representation.* The Offeror represents that—

(1) It □ will, □ 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. The Offeror shall provide the additional disclosure information required at paragraph (e)(1) of this section if the Offeror responds "will" in paragraph (d)(1) of this section; and

(2) After conducting a reasonable inquiry, for purposes of this representation, the Offeror represents that—

It □ does, □ does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services. The Offeror shall provide the additional disclosure information required at paragraph (e)(2) of this section if the Offeror responds "does" in paragraph (d)(2) of this section.

(e) *Disclosures.*

(1) Disclosure for the representation in paragraph (d)(1) of this provision. If the Offeror has responded "will" in the representation in paragraph (d)(1) of this provision, the Offeror shall provide the following

information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the original equipment manufacturer (OEM) or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable);or

(B) If not associated with maintenance, the Product Service Code (PSC) of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(1) of this provision.

(2) Disclosure for the representation in paragraph (d)(2) of this provision. If the Offeror has responded "does" in the representation in paragraph (d)(2) of this provision, the Offeror shall provide the following information as part of the offer:

(i) For covered equipment—

(A) The entity that produced the covered telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known);

(B) A description of all covered telecommunications equipment offered (include brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); and

(C) Explanation of the proposed use of covered telecommunications equipment and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(ii) For covered services—

(A) If the service is related to item maintenance: A description of all covered

telecommunications services offered (include on the item being maintained: Brand; model number, such as OEM number, manufacturer part number, or wholesaler number; and item description, as applicable); or

(B) If not associated with maintenance, the PSC of the service being provided; and explanation of the proposed use of covered telecommunications services and any factors relevant to determining if such use would be permissible under the prohibition in paragraph (b)(2) of this provision.

(End of provision)

FAR 52.204-26 Covered Telecommunications Equipment or Services-Representation (OCT 2020)

Definitions. As used in this provision, "covered telecommunications equipment or services" has the meaning provided in the clause 52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

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

Representation. The Offeror represents that it does, does not provide covered telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(End of provision)

FAR 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 30 days of contract expiration date.

(End of clause)

FAR 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 12 months; 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 60 months.

(End of clause)

HSAR 3052.204-71 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.

(End of clause)

ALTERNATE I (JULY 2023)

When the contract will require Contractor employees to have access to information resources, add the following paragraphs:
(g) Before receiving access to information resources under this contract, the individual must complete a security briefing; additional training for specific categories of CUI, if identified in the contract; and any nondisclosure agreement furnished by DHS. The Contracting Officer's Representative (COR) will arrange the security briefing and any additional training required for specific categories of CUI.
(h) The Contractor shall have access only to those areas of DHS information resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information resources not expressly authorized by the terms and conditions in this contract, or as approved in writing by the COR, are strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.
(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for DHS. It is not a right, a guarantee of access, a condition of the contract, or government-furnished equipment (GFE).
(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.
(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management, or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:
(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
(2) The waiver must be in the best interest of the Government.
(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)

ALTERNATE II (JULY 2023)

When the Department has determined contract employee access to controlled unclassified information or Government facilities must be limited to U.S. citizens and lawful permanent residents, but the contract will not require access to information resources, add the following paragraphs:
(g) Each individual employed under the contract shall be a citizen of the United States of America, or an alien who has been lawfully admitted for permanent residence as evidenced by a Permanent Resident Card (USCIS I-551). Any exceptions must be approved by the Department's Chief Security Officer or designee.

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

(End of clause)

HSAR 3052.209-72 Organizational Conflict of Interest (JUN 2006)

(a) Determination. The Government has determined that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting includes circumstances where Contractor personnel will likely investigate allegations and/or complaints pertaining to medical care issues within DHS Components. Contractor personnel either currently providing work for a DHS Component that is the same or similar in scope to the requirement under this contract, or who have provided the same or similar work for a DHS Component in the three years prior to the start of this contract, are not eligible to perform services on this contract in order to prevent the existence or appearance of conflicting roles that might affect a contractor's judgement.

(b) If any such conflict of interest is found to exist, the Contracting Officer may

(1) disqualify the offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the offeror and include the appropriate provisions to avoid, neutralize, mitigate, or waive such conflict in the contract awarded. After discussion with the offeror, the Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the offeror may be found ineligible for award.

(c) Disclosure: The offeror hereby represents, to the best of its knowledge that:

_(1) It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this contract, or

_(2) It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included a mitigation plan in accordance with paragraph (d) of this provision.

(d) Mitigation. If an offeror with a potential or actual conflict of interest or unfair competitive advantage believes the conflict can be avoided, neutralized, or mitigated, the offeror shall submit a mitigation plan to the Government for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan.

(e) Other Relevant Information: In addition to the mitigation plan, the Contracting Officer may require further relevant information from the offeror. The Contracting Officer will use all information submitted by the offeror, and any other relevant information known to DHS, to determine whether an award to the offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

(f) Corporation Change. The successful offeror shall inform the Contracting Officer within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

(g) Flow-down. The contractor shall insert the substance of this clause in each first tier subcontract that exceeds the simplified acquisition threshold.

(End of provision)

HSAR 3052.209-73 Limitation of Future Contracting (JUN 2006)

(a) The Contracting Officer has determined that this acquisition may give rise to a potential organizational conflict of interest. Accordingly, the attention of prospective offerors is invited to FAR Subpart 9.5 - Organizational Conflicts of Interest.
The nature of this conflict is that this effort may result in an actual or potential conflict of interest, or may provide one or more offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting includes circumstances where Contractor personnel will likely investigate allegations and/or complaints pertaining to medical care issues within DHS Components. Contractor personnel either currently providing work for a DHS Component that is the same or similar in scope to the requirement under this contract, or who have provided the same or similar work for a DHS Component in the three years prior to the start of this contract, are not eligible to perform services on this contract in order to prevent the existence or appearance of conflicting roles that might affect a contractor's judgement.

(b) The restrictions upon future contracting are as follows:

(1) If the Contractor, under the terms of this contract, or through the performance of tasks pursuant to this contract, is required to develop specifications or statements of work that are to be incorporated into a solicitation, the Contractor shall be ineligible to perform the work described in that solicitation as a prime or first-tier subcontractor under an ensuing DHS contract. This restriction shall remain in effect for a reasonable time, as agreed to by the Contracting Officer and the Contractor, sufficient to avoid unfair competitive advantage or potential bias (this time shall in no case be less than the duration of the initial production contract). DHS shall not unilaterally require the Contractor to prepare such specifications or statements of work under this contract.

(2) To the extent that the work under this contract requires access to proprietary, business confidential, or financial data of other companies, and as long as these data remain proprietary or confidential, the Contractor shall protect these data from unauthorized use and disclosure and agrees not to use them to compete with those other companies.

(End of clause)

3052.212-70 Contract Terms and Conditions Applicable to DHS Acquisition of Commercial Items (SEP 2012)

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.
(b) Clauses.

__3052.203-70 Instructions for Contractor Disclosure of Violations.
__3052.205-70 Advertisement, Publicizing Awards, and Releases.
__3052.209-73 Limitation on Future Contracting.
__3052.228-70 Insurance.
__3052.236-70 Special Provisions for Work at Operating Airports.
__3052.247-70 F.o.B. Origin Information.
__Alternate I
__Alternate II
__3052.247-71 F.o.B. Origin Only.
__3052.247-72 F.o.B. Destination Only.

(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:
Medical Doctor Subject Matter Expert

Section IX – INSTRUCTIONS, CONDITIONS AND NOTICES

(This section will be removed after award)

1 PROPOSAL DUE DATE AND DELIVERY

The Offeror shall submit its Proposal via email to the Contracting Officer (CO),

The Contracting Officer and the Contract Specialist will perform an initial compliance check of Proposals to determine conformance of the Proposal to the RFP instructions. Proposals found to be in gross non-conformance with the RFP instructions will be identified by the CO and may be excluded from the competition.

An Offeror that does not meet the delivery deadline for receipt may be excluded from the competition and its Proposal may not be accepted.

2 QUESTIONS AND AMENDMENTS

All questions regarding this RFQ must be submitted in writing to the Contracting Officer,

Questions asked over telephone or voicemail will not be accepted as formal questions for this requirement and will not be addressed in any amendments to the RFP.

The Government recommends that the Offeror ensure that questions are written to enable a clear understanding as to the Offeror's issues or concerns with the referenced area of the solicitation. Statements expressing opinions, sentiments, or conjectures are not considered valid inquires or comments for this purpose and will not receive a response from the Government.

The Government will consolidate all responses to vendor questions into an amendment and issue the amendment to all Offerors.

3 PROPOSAL CONTENT

The proposals shall consist of two volumes. Volume I shall be the technical proposal and Volume II shall be the price proposal.

Naming Convention	**Tab Title**
Volume I: Technical	
Tab A	Quotation Cover/Transmittal Letter (Limit 1 page)
Tab B	Technical Quotation (Limit 25 Pages) Past Performance (Attachment A, Limit 9 Pages)
Note: Volume I Technical 25-page limit excludes the quotation cover/transmittal letter; resumes; letter of commitment and completed Past Performance Information Form and any CPARs assessment reports. In addition, although not required, a title page or table of content is also excluded if the Quoter chooses to submit.	

Volume I: Technical Proposal Content

Offerors' technical proposals shall include sections entitled Technical Capability and Past Performance; each section shall address all technical evaluation criteria. Offerors shall provide specific and detailed responses to all technical requirements. The proposals shall clearly demonstrate Offerors' understanding of the overall requirement and tasks and convey Offerors' ability to provide the required services. Simple statements of compliance without detailed description of how Offerors will comply with the requirement, may not be considered sufficient evidence that the Offeror can technically meet the requirements of this RFP. Technical proposals that merely restate the Government's requirements are unacceptable and shall result in adverse technical ratings.

The Offeror's technical submission must demonstrate the firm's capability to perform the requirements outlined in the solicitation. The Offeror shall provide a technical proposal that addresses the following two (2) criterias:

Factor #1: Technical Capability and Understanding

Offerors shall:

1) Provide a narrative explaining how the experience of the personnel who will perform work on this Contract meets or exceeds the technical requirements as stated in Section II of this solicitation.

2) A narrative description of the knowledge the personnel have gained through completed and ongoing efforts that are similar in nature to the solicitation requirements as stated herein.

3) Provide resumes (limited to five (5) pages per resume) for all personnel who will perform on this contract. The resumes shall include, at a minimum, the personnel's name, a detailed description of the personnel's professional background/qualifications, skills, education, accomplishments, and work experience as it relates to this acquisition and as identified in Section II – Statement of Work.

Factor # 2: Past Performance

Offerors shall identify a minimum of three (3) ongoing or completed professional projects/contracts/orders that demonstrate recent and relevant past performance. Relevant is defined as work similar in size, scope, and complexity to the services identified in this solicitation. Recent is defined as work within the last three (3) years from receipt of this solicitation. Past performance reports may be accessed by the Government through the Past Performance Information Retrieval System (PPIRS) at https://www.ppirs.gov. The Government may also use present and/or past performance data obtained from various sources in addition to the information provided with the technical proposal. Technical evaluators may also use personal knowledge of Offerors' past performance.

Offerors shall provide the following past performance information:

- Project title and location/address.
- Name and title of the client's point of contact (i.e. CO and COR, etc.) and contact information (i.e. telephone, email address).
- Government agency or company/organization for whom services were provided.
- Contract/order number

- Contract/order award and final amount.
- Date of contract/order award and completion.
- Brief description of services.
- Key personnel - Please identify the individual(s) who worked on the projects and are proposed for this requirement.
- Brief description of problems encountered and corrective actions. Offerors shall specifically address and clarify past unfavorable reports.
- A brief narrative of why the Offeror believes this reference is relevant to the proposed task.

Offerors shall forward the Past Performance Questionnaire, Attachment A, to the Offeror's references. The references shall then submit their completed questionnaire directly to the Contracting Officer, Contracting Officer,
Questionnaires shall not be delivered directly from the Offeror.

Volume II – Price Proposal Content

Volume II: Business & Pricing	
Tab A	Quotation Cover/Transmittal Letter (Limit 3 pages)
	FAR 52.204-24 Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment (d) *Representation*
	Price Quote (utilize the schedule on pages 3-4 under SECTION 1 – SUPPLIES OR SERVICE/PRICES)

Factor #3: Price

The Offeror shall include the following information in the cover letter of its price quotation:

- Dun & Bradstreet Number (DUNS)
- Unique Entity ID (UEI)
- Contact Name
- Contact Telephone and E-mail Address
- Complete Business Mailing Address

In its price quotation, the Offeror shall:

- Identify any contractors it plans to subcontract with for this procurement.
- Submit a completed Pricing Sheet of this solicitation, which requires the Offeror to complete the proposed price for each CLIN in the schedule on pages 3-4 under SECTION 1 – SUPPLIES OR SERVICE/PRICES.
- Complete and submit the certification required in Section VII of this solicitation.
- As part of Volume II, the Offeror shall provide a completed copy of all solicitation provisions that require the Offeror's input.
  (i) Present an adequate accounting system. The offeror's accounting system must substantiate vouchers (including any subcontractor hours reimbursed at the hourly rate in the schedule) by evidence of actual payment and by: Individual daily job timekeeping records;
  (ii) Records that verify the employees meet the qualifications for the labor categories specified in the contract; and
  (iii) Other substantiation requested by the CO. (FAR 52.232-7(a)(5)).

Offeror must provide in proposal:

- If requested, the offeror will provide sufficient accounting system information to allow a pre-award accounting system review for adequacy

Section X – EVALUATION CRITERIA FOR AWARD

(This section will be removed after award)

1.0 BASIS FOR AWARD

For each evaluation criteria, the Government will assess its level of confidence that the Offeror will successfully perform the requirements of the SOW.

Awards will be made to the responsible Offeror submitting an overall proposal that is determined most advantageous to the Government, price and non-price factors considered. Awards will be made to the firm whose proposal meets the Government's requirements and whose technical evaluation and price represents the best value to the Government. The evaluation criteria of 1) Technical Capability and Understanding and 2) Past Performance are of descending importance and when combined are significantly more important than Price. Price may become the determining factor for award as quotations become more equal based on other factors.

The Government will not make an award at a significantly higher overall price to the Government to achieve only slightly superior technical capability. The Government will conduct a tradeoff analysis that involves the assessment of benefits of superior technical capability features (i.e., benefits clearly attributable to increased productivity, probability of successful task order performance, and/or unique and innovative approaches or capabilities) versus the added price, as necessary.

In the event that two or more proposals are determined not to have any substantial technical differences (i.e. are technically equivalent), award may be made to the lower priced proposal. It should be noted that award may be made to other than the lowest priced proposal 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 quotation, if the Government determines that a price premium is not warranted.

The Government reserves the right to award on initial offers; therefore, each Offeror shall include the most favorable and advantageous price, technical, and past performance that the Offeror can submit to the Government. However, the Government may conduct negotiations with firms, if warranted.

2.0 VOLUME 1-TECHNICAL PROPOSAL EVALUATION

Evaluation Factor 1 - Technical Capability and Understanding

The Government will evaluate the Offeror's Technical Capability by evaluating the extent to which the Offeror:

1) Provides a narrative explaining how the experience of the personnel who will perform work on this Contract meets or exceeds the technical requirements as stated in **Section II** of this solicitation.

2) Provides a narrative description of the knowledge the personnel has gained through completion and ongoing efforts that are similar in nature to the solicitation requirements as stated herein.

3) Provides resumes (limited to five (5) pages per resume) for all personnel who will perform on

this contract. The resumes shall include, at a minimum, the personnel's name, a detailed description of the personnel's professional background/qualifications, skills, education, accomplishments, and work experience as it relates to this acquisition and as identified in Section II – SOW.

Evaluation Factor 2: Past Performance

Past Performance will be evaluated to determine how well the Offeror has performed in the recent past (3 years) as an indicator of how well the Offeror may perform in the future. Past Performance must be relevant, which is work similar in size, scope and complexity. If an Offeror has no relevant past performance, the Offeror must state this in the quotation. If an Offeror includes in its quotation past performance that is not relevant, the government may consider this to demonstrate that the Offeror does not have a clear understanding of the SOW.

The Government reserves the right to use publicly available reports and data from the Past Performance Information Retrieval System (PPIRS) found on the web at http://www.ppirs.gov/. The Government may also use present and/or past performance data obtained from a variety of sources, not just those contracts identified by Offerors. Technical evaluators may also use personal knowledge of Offerors' past performance. An Offeror without a record of past performance or for whom information on relevant past performance is not available will not be evaluated favorably or unfavorably.

3.0 VOLUME II-PRICE PROPOSAL

Evaluation Factor 3 – Price

The Government will conduct a price analysis by (a) comparing the proposed prices received in response to this solicitation, and (b) comparing the proposals against an Independent Government Cost Estimate Price analysis will be conducted to determine the reasonableness of the Offeror's proposed price. The Government will also evaluate the option periods in accordance with FAR 52.217-5 Evaluation of Options (JUL 1990): Except when it is determined in accordance with FAR 17.206(b) not to be in the Government's best interests, the Government will evaluate proposals for award purposes by adding the total price for all options to the total price for the basic period. A determination of an adequate accounting system is required for award and contract performance.

If needed, the Government intends to exercise the option or options under FAR 52.217-8 without further competition or need for a limited source justification. For purposes of evaluation, the potential need to exercise the option under FAR 52.217-8 to extend the period of contract performance for the maximum period of six (6) months beyond the last option period will be considered the same for all Offerors. In considering the price of the base period and any option periods, the Government will consider that if the extension of service clause (FAR 52.217-8) is exercised, it will be on the exact same rates and terms, other than length of performance, as the base or option period being extended.

The Government will determine whether the price, inclusive of all options (including the options available under FAR 52.217-8), is fair and reasonable, and whether the price of the base period and all option periods (including the option(s) represented by FAR 52.217-8), in combination with the other evaluation criteria specified in the solicitation, represents the best value to the Government. Evaluation of options will not obligate the Government to exercise the option(s).