DEPARTMENT OF HOMELAND SECURITY (DHS)
Science & Technology Directorate (S&T)
Office of Enterprise Services (OES)
Diversity, Equity, Inclusion, & Accessibility (DEIA) Office
STATEMENT OF WORK (SOW)
FOR Communication Access Services (CAS)
American Sign Language (ASL) Interpretation Services

August 2023

1.0 GENERAL

1.1 BACKGROUND

The Department of Homeland Security (DHS) Science & Technology (S&T) Directorate, Office of the Enterprise Services (OES) Diversity, Equity, Inclusion, & Accessibility (DEIA) Office has a need for American Sign Language (ASL) Interpretation Support Services to support the accommodation needs of employees who require such services.

1.2 SCOPE

The scope includes language and communication devise services for the deaf, hard of hearing, and blind communities to support S&T with reliable, efficient, and effective virtual and on-site (at any location within the United States and its territories) interpretation services.

S&T requires sign language interpretation to help support communication access and ensure equal opportunity for individuals who are employed by S&T and those who are served or encountered in S&T programs and activities. The Contractor shall provide sign language interpretation. Sign language interpretation is visual communication that provides interpretation and translation of spoken words to and from individuals using a sign language system in various situations including in-person meetings, or via VRI. S&T requires Video Remote Interpretation (VRI) services to help support communication and ensure equal opportunity for individuals who are employed by S&T and those who are served or encountered in S&T programs and activities as an option when in-person, on-site interpreting services are not immediately available. Contractors providing VRI services must have the same certification requirements as on-site language interpreters. The Contractor shall be able to use and provide videoconferencing technology, equipment, and a high-speed internet connection with sufficient bandwidth to provide the interpretation services of an interpreter from one location to people at a different location(s).

S&T also requires Communication Access Realtime Translation (CART) services to help support effective communication access and ensure equal opportunity for individuals who are employed by DHS and those who are served or encountered in DHS programs and activities. Also known as "real-time captioning" or "Computer Aided Real Time Translation" services, CART service is defined by the National Court Reporters Association (NCRA) as "the instant translation of the spoken word into English text using a stenotype machine, notebook computer and Realtime

software. The text appears on a computer monitor or other display." It is a "word-for-word speech-to-text interpreting service for people who need communication access and benefits people who are late-deafened, oral deaf, hard of hearing, or who have cochlear implants." The Contractor shall be able to use and provide required CART equipment and software to provide the interpretation service of a nationally certified Realtime/Court Reporter in variety of settings to different sizes of groups and types of audiences. CART services are required within and outside government facilities. Upon request, transcripts shall be made available following the provision of CART services.

1.3 OBJECTIVE

The Contractor objective is to provide in-person virtual and on-site (when needed) interpreting services between spoken English and ASL by specially trained sign language interpreters, as well as those who require further language support and VRI for offsite interpreter relaying information regardless of where the Deaf and hearing customers are located. The Contractor shall provide CART Services that transcribes speech into text that can be viewed on a laptop, projection screen,or television monitor as needed.

1.4 APPLICABLE DOCUMENTS

(a) Ordering Guide for Communication Access Services (CAS). The CAS BPA is for: Services for the Deaf, Hard of Hearing, and Blind Communities includes sign language interpretation. Video Remote Interpretation (VRI), Communication Access Realtime Translation (CART), Braille transliteration, reader services, and desktop publishing services and 508 compliance. Version 1 dated November 7, 2022.

1.4.1 Reference Documents

The following documents may be helpful to the Contractor in performing the work described in this document:

(a) DHS CAS BPA Terms and Conditions
(b) Contractor's BPA Staffing and Recruitment Plan
(c) FTR (Federal Travel Regulation) http://www.gsa.gov/portal/content/104790

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 SIGN LANGUAGE INTERPRETER (SLI) SERVICES

The Contractor shall provide interpreters on an ad hoc by request basis. Ad hoc service shall be provided virtually or on-site as designated in the request. On-site interpreters may be required to provide services anywhere in the US. However, requests for on-site services will primarily be required in the National Capital Region (NCR) at any site associated with the execution of S&T work.

2.1.1 Task 1 – SIGN LANGUAGE INTERPRETATION (SLI) SERVICES In-Person

2.1.1.1 The Contractor shall provide qualified personnel to perform sign language interpretation services for S&T employees and customers on an on-call basis, in accordance with this Statement of Work (SOW) during the business hours of 7:30 am-6:00 pm, Monday through Friday.

2.1.1.2 The on-site service shall be provided as required at the designated locations within National Capital Region (NCR). Requests shall be made by the Program Manager (PM), Contracting Officer Representative (COR), or named employees receiving SLI services. **The Contractor shall make every attempt to provide on-site (NCR) interpreters on all requests received 24 hours prior to the date/time the services are to be provided and will provide video interpretation services if no onsite interpreter is available.**When the Government is unable to provide the stated 24-hour notice, the Contractor shall have the right to indicate that the request cannot be fulfilled due to insufficient notice. However, the Contractor shall make a good faith attempt to fulfill the request if possible. The Contractor's inability to fulfill the request based on insufficient notice must be given within two (2) hours of the time the request was placed during the business day. Upon acceptance of a request, the Contractor shall provide the PM, COR, and/or the employee receiving SLI services the name(s) of the interpreter(s) as soon as possible or at a minimum of four (4) hours prior to the service being provided.

2.1.1.3 The sign language interpreter must possess the ability to sign, voice to sign, and sign to voice, in many different situations including but not limited to meetings, platforms, conferences, small groups and large groups.

2.1.1.4 The Contractor shall coordinate a schedule with the COR or alternate POC to ensure at least 2 interpreters are available for events lasting greater than or equal to one hour (1.0) hour to assist Deaf and or hearing- impaired employees or customers at meetings or conferences requiring interpreter service.

2.1.1.5 The Sign Language Interpreter (SLI) shall be responsible for interpreting phone calls and interactions between employees and office staff, ensuring the information is disseminated to employees through a variety of interpreting techniques tailored to the employee's needs.

2.1.1.6 The Contractor shall have the ability to travel with the DHS employee to local meetings, conferences, and trainings in a variety of locations within the within National Capital Region (NCR).

2.1.1.7 The Contractor shall provide SLI interpreter services outside of the NCR when requested by the Government. The Government shall provide no less than 14 calendar days' notice to the Contractor to allow the Contractor to make arrangements to support the request. The Contractor must provide an acknowledgement of the request within 24 hours and coordinate with the COR and employee who will be traveling to ensure appropriate coordination of travel plans and service scheduling.

2.1.1.8 The Contractor shall provide SLI services both On-Call and through Reservation Scheduling.

2.1.2 Coordinating and Scheduling Interpreter Requests

The PM, COR, or the employee receiving SLI services shall be responsible for coordinating and scheduling interpreter requests. The PM, COR, or the employee

receiving SLI services shall contact the Contractor primarily via email, and secondarily via telephone, with requests for, changes to, or cancellations of interpreter services. The PM, COR, or the employee receiving SLI services shall provide pertinent information related to the assignment, including date, time, projected length of assignment, type of assignment, location, on site POC, on site POC phone number, sign language preference if other than ASL.

2.1.3 The PM, COR, or the employee receiving SLI services shall contact the Contractor primarily via email, and secondarily via telephone, with requests for changes to, or cancellations of interpreter services.

2.2 Task 2 – VIDEO REMOTE INTERPRETATION (VRI)

The PM, COR, or the employee receiving SLI services shall be responsible for coordinating and scheduling Video Remote Interpretation requests, this is a video-telecommunications service that uses devices such as web cameras or videophones to provide sign language or spoken language interpreting services. The PM, COR, or the employee receiving SLI services shall contact the Contractor primarily via email, and secondarily via telephone, with requests for, changes to, or cancellations of Video Remote Interpretation services. The PM, COR, or the employee receiving SLI services shall provide pertinent information related to the assignment, including date, time, projected length of assignment, type of assignment, location, on site POC, on site POC phone number, and Video Remote Interpretation preference if other than ASL.

2.2.1 The Contractor shall provide on-demand Video Remote Interpreting (VRI) sign language interpretation service delivered over a live high-quality video and audio internet connection.

2.2.2 The Contractor shall provide a secured Advanced Encryption Standards (AES) encryption or other functionally equivalent secured site.

2.2.3 The Contractor shall provide qualified SLI to provide the VRI service.

2.2.4 When accessing VRI services, interpreters must be located within the continental United States and its territories (i.e. Puerto Rico, Guam, etc.).

2.2.5 The Contractor shall ensure each interpreter be identified by a unique code that the Contractor has assigned to maintain confidentiality. Other coding may be required to identify government office location or personnel, as specified in individual orders. The Contractor shall meet additional requirements as specified in each order specified by Components.

2.2.6 The VRI service shall be available during normal hours of operation where offices are located between the hours of 6:30 am and 6:00 pm, Monday through Friday, in all time zones.

2.2.7 The VRI service shall be available for both scheduled and ad-hoc services within 1 hour of the user's request for service.

2.2.8 The Contractor shall provide the user with a time estimate for an interpreter at the time the initial point user requests service. The wait time for an interpreter shall not be greater than 10 minutes.

2.2.9 The Contractor shall provide an operator assistance service to assist the user with any connectivity issues between the Agency and the Contractor.

2.2.10 The Contractor shall provide a toll-free telephone number whereby the user can connect with the operator assistance service if the VRI connection is unsuccessful.

2.2.11 The Contract shall ensure the VRI service is compatible with the Agency's technical requirements and not make any changes to the VRI service provided that would have an impact on the Agency's ability to connect to the Contractor 's VRI service.

2.2.12 The Contractor shall provide instructional materials for users demonstrating how the user can use Agency equipment to connect to the Contractor and initiate VRI service.

2.2.13 The Operator shall have the capability to track each incoming connection, by capturing the incoming telephone number via Caller ID and the user's name. The Contractor shall also have in place automated equipment (i.e., caller identification) to capture the incoming telephone number for each connection to serve as a cross check on the office codes provided by Agency employees.

2.2.14 The Contractor shall provide a backup plan to provide VRI services in the event of Contractor system problems, disasters, natural or otherwise, or any other outage that would impact the Agency's ability to connect to the Contractor for VRI services.

2.2.15 The Contractor shall assign each interpreter a unique identifier (i.e., operator number ###). At the beginning of each connection, the interpreter shall provide the user with his or her unique identifier.

2.2.16 The Contractor shall ensure that all interpreters have signed the necessary non-disclosure statements about information relayed during the VRI session.

3.0 Task 3 – COMMUNICATION ACCESS REALTIME TRANSLATION (CART)

The PM, COR, or the employee receiving SLI services shall be responsible for coordinating and scheduling Communication Access Realtime Translation (CART) requests. This is an instantaneous translation of the spoken language into text and displayed in various forms. The PM, COR, or the employee receiving SLI services shall contact the Contractor primarily via email, and secondarily via telephone, with requests for changes to, or cancellations of CART services. The PM, COR, or the employee receiving SLI services shall provide pertinent information related to the assignment, including date, time, projected length of assignment, type of assignment, location, on site POC, on site POC phone number, CART preference if other than ASL.

3.1.1 The Contractor shall provide onsite or remote offsite Communication Access Real-time Transcription (CART) services including but not limited to:

3.1.1.1 Translates spoken word into English text using a stenotype machine, notebook computer and Realtime software. Materials include but are not limited to: Business, Legal, Medical, Technical, Documents, Software, Website localization for Internet and Intranet, Video subtitling, captioning, and Transcriptions for Title III Monitoring. Include translation formatting, proofreading, text adaptation, editing, graphic design, and desktop publishing.

3.1.2 If the Government requires remote offsite CART services the Contractor shall work with the Government to determine the IT requirements in advance, such as firewall and closed-captioning issues, etc.

3.1.3 The Contractor shall provide a Certified Real-time Reporter or a Certified CART Provider.

3.1.4 The Contractor shall bring onsite his or her own laptop computer, stenotype machine, and real-time software to produce text to be displayed on a computer or projected on a screen.

3.1.5 For remote CART services, the Contractor shall have their own computer with a reliable high-speed Internet connection and a wireless microphone in the room where the meeting or event is taking place.

3.1.6 The Contractor shall ensure that once a job is confirmed, the assigned Certified Real-time Report or Certified CART Provider shall stay with the job unless replaced by another Certified Real-time Reporter or Certified CART Provider.

3.1.7 The PM or the COR or receiving employee shall be responsible for coordinating and scheduling services and/or support.

3.2 Task 4 – SURGE SUPPORT (OPTIONAL)

The government anticipates that there may be additional support requirements for this task order as DHS hiring conditions evolves. A minimum notice of thirty (30) days shall be provided to the Contractor prior to ordering and funding surge support line item(s). When operational conditions require additional staffing, the Contractor shall provide additional support as requested by the government. Surge support shall not be provided until the Surge Contract Line-Item Number (CLIN) has been exercised and funded. When such support is required, the government shall specify the work to be performed and duration of assignment.

4.0 CONTRACTOR PERSONNEL

4.1 **Qualified Personnel**. The Contractor shall provide qualified personnel to perform all requirements specified in this SOW. All Contractor personnel providing services under this BPA shall meet the minimum qualifications and proficiency levels set forth in CAS Attachment A based on the applicable linguist tiered level set forth in orders. The Contractor shall ensure all minimum personnel qualifications are met prior to providing any services under this BPA.

Minimum personnel qualification: Tier 2 with no certification via in-house testing. Note: All ASL interpreters for this requirement should have a Registry of Interpreters for the Deaf level NIC Advanced or Master or (RID) Comprehensive Skills Certification (CSC) or equivalent state level certification. All interpreters shall conduct themselves according to the RID Code of Professional Ethics.

The Contractor shall present proof of linguist specialists' qualifications and proficiency testing upon request of the Component Contracting Officer. In extraordinary cases, the Contractor may request a waiver of this requirement on an individual language specialist basis providing detailed justification for such a waiver in each case. The waiver request must be approved by the Component CO issuing the order.

The primary mode of sign language interpreting shall be translation between English-like signing and spoken English and/or interpreting between American Sign Language and spoken English, or translate Pidgin Signed English (PSE), Signed Exact English (SEE) or tactile sign language. If requested, the Contractor must provide a sign language interpreter with strong voicing skills. Sign language interpreters are to conduct themselves in a professional manner.

All ASL interpreters for this requirement should have a Registry of Interpreters for the Deaf level NIC Advanced or Master or (RID) Comprehensive Skills Certification (CSC) or equivalent state level certification
Sign Language Interpretation and Video Remote Interpreting (VRI)

- Minimum Requirements for Sign language interpreters, must be:
  - Be 18 years old or older;
  - Hold a high school diploma or equivalent;
  - Be a U.S. citizen or a foreign national who has been lawfully admitted for permanent residence; however, if the Contractor will access the DHS network or intranet, they must be a U.S. citizen;
  - Fluency in American Sign Language (ASL) or requested system depending on the effective communication access needed by the orders;
  - Be certified/qualified in interpreting English to ASL, or other sign system, and translating from ASL, or other sign system, to English;
  - Have a minimum of three years of experience that involved translating and interpreting through the use of ASL or other sign system depending on the effective communication access needed by the orders
  - Have a minimum of one year of experience that involved training program development, evaluation, or instruction in a program of training;
  - Be registered with the Registry of Interpreters for the Deaf (RID) or hold a certification of NIC (National Interpreter Certification) or CDI (Certified Deaf Interpreter) or have a state-equivalent certification/licensure; and
  - Comply with the Code of Professional Conduct established by RID or state professional ethics established by the states.

- Additional Requirements as specified in orders. For example, additional requirements may include: Have knowledge of vocabulary as it relates to persons with disabilities in the emergency management field. (see CAS Attachment B)
  - Have training or certification in legal interpreting/mental health/medical interpreting.

- Communication Access Realtime Translation (CART)
  - Minimum Requirements, must:
    - Be 18 years old or older;
    - Hold a high school diploma or equivalent;
    - Be a U.S. citizen or a foreign national who has been lawfully admitted for permanent residence; however, if the Contractor will access the DHS network or intranet, they must be a U.S. citizen;
    - Have at least three years' work experience with individuals who are Deaf or Hard of Hearing in a professional setting to be documented;
    - Must have one of the following certifications from NCRA or equivalent:
      - CRR-Certified Realtime Reporter
      - CCP-Certified CART Reporter
      - CBC-Certified Broadcast Captioned
    - Able to interpret and transcribe terminology including but not limited to technical terminology, laws, regulations, concepts, practices, legal

terminology, etc. pertaining to criminal investigation, forensic services, treasury obligation, personnel & payroll operation. A working knowledge of acronyms used by the DHS and its Components; and

- Must possess knowledge of Deaf and Hard of Hearing Community and Deaf Culture.

4.2 NUMBER OF INTERPRETERS REQUIRED PER ASSIGNMENT

The number of interpreters required is subject to the approval of the COR. In general, two (2) interpreters shall be required for assignments lasting more than two (2) hours; requiring detailed or technical interpreting; or involving general audiences that last more than one (1) hour.

4.3 ARRIVAL OF INTERPRETERS

All interpreters must have a valid government issued photo ID. The COR shall provide the Contractor with the requirements regarding accepted photo IDs. Interpreters shall arrive not later than fifteen (15) minutes prior to a scheduled assignment regardless of where the assignment is located. The Contractor shall bill the agency for any of the time described in this paragraph.

4.4 REASSIGNMENT OF AD HOC INTERPRETER(S) AS NEEDED

If an ad hoc interpreter is on-site for a scheduled assignment open to a general audience and no one requiring interpreter services is in attendance, the interpreter shall contact the PM and the COR located within the designated facility fifteen (15) minutes after the start of the event. The COR has the option to assign the interpreter to another request without an additional charge/cancellation fee with the stipulation that if the new assignment is of similar size, scope, and location as the original request, differences in size, scope, and location shall be charged. If the event is being videotaped, the interpreter shall provide interpreting services whether or not there are people in attendance requiring interpreter services.

4.5 CLOSURE OF FEDERAL GOVERNMENT DUE TO INCLEMENT WEATHER OR EMERGENCY

Interpreters shall not be required to physically report to work if the federal government is closed due to inclement weather or emergency. No cancellation fee or charges shall be assessed. The Contractor shall not bill the government for interpreter service hours when the government is closed due to inclement weather or emergency. However, in the event that the federal government physical offices are closed but employee(s) are still required to work remotely, either the PM, COR, or the employee receiving SLI services shall be responsible for coordinating and scheduling VRI requests as soon as they are aware of the requirement.

4.6 **OTHER UNSCHEDULED FEDERAL GOVERNMENT CLOSURES**

In the event of an unscheduled closure of the federal government interpreters shall not report to work or to their scheduled assignments. Cancellation fees or charges shall be assessed if cancellation is less than 48 hours from the schedule time of service. The Contractor shall not bill the government for interpreter service hours when the government is closed.

4.7 **FEDERAL HOLIDAYS**

Interpreter services may be required on federal holidays and weekends during a

disaster declaration and the contract can bill for the services received

4.8 **INCLEMENT WEATHER- NON-CLOSURES**

In the event of severe inclement weather or an emergency, interpreter (is responsible for calling one or both of the requesting organization's POCs at the numbers provided on their assignment document or the COR to determine if the assignment is still scheduled. The interpreters shall abide by the OPM delay arrival policy pertaining to Federal employees at each identified work facility. If the interpreter services have been canceled, the Contractor may assess the cancellation fee for requests for services that are canceled with less than 4 hour's notice. If the interpreter service is still required, and the Contractor is not able to provide the service, the Contractor shall not bill the government for interpreter service hours when required service is not provided.

4.8.1 In the event any or all of the on-call interpreters are unable to come to work, the Contractor is required to notify the requesting organization's point of contact (POC). The Contractor shall be required to replace the interpreter(s). In the event, the Contractor is unable to supply the Agency with replacement interpreters; the Contractor shall not bill the government for interpreter service when the Contractor is not able to provide the interpreters.

4.9 REIMBURSEMENT FOR NON-AD HOC and- AD HOC INTERPRETER REQUESTS

Regardless of assignment duration, the Contractor shall be reimbursed for a minimum of two (2) hours. Assignments lasting more than two (2) hours shall be invoiced for the actual estimated duration requested by the PM, COR, or the employee receiving SLI services when coordinating and scheduling the request. For billing purposes, the Contractor shall round up to the nearest half-hour. For assignments lasting more than eight (8) continuous hours, the Contractor shall be reimbursed at the rate of 1.5 times the hourly rate established in the Pricing Schedule for the portion of the assignment that exceeds 8 hours. For example, if an assignment last ten (10) hours, the Contractor shall bill for eight (8) hours using the established hourly rate and two (2) hours at the hour rate multiplied by the 1.5 factor.

5.0 CANCELLATION OF ASSIGNMENT -INTERPRETER

The PM, COR or the employee receiving SLI services shall contact the Contractor primarily via email, and secondarily via telephone, for cancellations of assignment requests.

5.1 Ad hoc/non-ad hoc service requests that are canceled with less than 48 hours of notice prior to the event shall be reimbursed for actual scheduled hours. Ad hoc/non-ad hoc service

requests canceled with more than forty-eight (48) hours of notice prior to the event shall not be reimbursed.

5.2 If an ad hoc/non-ad hoc interpreter service request is canceled less than forty-eight (48) hours prior to the event, the PM, COR, or the employee receiving SLI services, and the Contractor can mutually agree to reassign the ad hoc interpreter to another interpreter service request covered by this SOW without incurring cancellation charges.

6.0 ASSIGNMENT LOG

The Contractor shall maintain a log of the dates an order was placed, the time the order was placed, the job number, the date of the assignment, the start time of the assignment, the anticipated duration and a description of the event for each assignment given to the Sign Language Interpreters. The log shall be made available to the COR as requested for inspection; however, the final assignment log shall be submitted with the invoice by the 10th of each month.

7.0 EVALUATION OF SERVICES

Recipients of interpreter services may provide feedback on the quality of the interpreter services received to the COR. This feedback shall be provided to the Contractor by the COR within 48 hours of receipt of the feedback. The Contractor shall take appropriate action based on the feedback and provide the COR with a response to the feedback within 24 hours of receipt of the feedback. The COR, along with the PM, and the Contractor shall meet periodically upon COR request to conduct a quality review of services being provided by the Contractor .

8.0 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is maintained at all times. The Contractor shall ensure that all contract support personnel are present for all hours of the workday. If for any reason the Contractor staffing levels are not maintained due to vacation, leave, appointments, etc., and replacement personnel shall not be provided, the Contractor shall provide e-mail notification to the COR prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

8.1 Key Personnel

Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer no less than 15 business days in advance, submit written justification for replacement, and provide the name and qualifications of any proposed substitute(s). All proposed substitutes shall possess qualifications equal to or superior to those of the *Key* person being replaced, unless otherwise approved by the Contracting Officer. The Contractor shall not replace *Key* Contractor personnel without approval from the Contracting Officer. The following Contractor personnel are designated as Key for this requirement. Note: The Government may designate additional Contractor personnel as *Key* at the time of award.

Project Manager

8.2 Employee Identification

In accordance with DHS's security policy, *"Post Award Instructions Regarding Security Requirements for Non-Classified Contracts/Orders"*, provided in Section 3.9 below, the Contractor shall coordinate with the COR to assure that any Contractor employee requiring access to the DHS offices has a Contractor identification/building pass before the employee enters on duty. Personnel designated by the COR shall complete appropriate forms specified by the DHS Office of the Chief Security Officer for security clearance requirements.

8.2.1 Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent and display all identification and visitor badges in plain view above the waist at all times.

8.2.2 Contractor employees working on-site at Government facilities shall wear a Government issued identification badge. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

8.3 Post Award Instructions Regarding Security Requirements for Non-Classified Contracts/Orders

- The procedures outlined below shall be followed for the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD) to process background investigations, Entry on Duty determinations, and Fitness 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 shall perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations shall be processed through the DHS OCSO/PSD. Prospective Contractor employees shall submit the below completed forms to the DHS forms to the DHS OCSO/PSD. The Standard Form (SF) 85-P must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85P signature pages and other completed forms must be given to the OSCO/PSD no less than thirty (30) days before the start date of the contract or thirty (30) days prior to the requested entry on duty date, for all Contractor employees whether a replacement, addition, subcontractor employee, or vendor:

a. Standard Form (SF) 85-P, "Questionnaire for Public Trust Positions"

i. SF-85P Certification
ii. SF-85P Authorization for Release of Medical Information

b. FD Form 258, "Fingerprint Card" (2 copies)
c. DHS Form 11000-6, "Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement"
d. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" Only complete packages shall be accepted by the DHS OCSO/PSD. Specific instructions on submission of packages shall be provided upon award of the contract.

8.4 Employee Conduct

Contractor's employees shall comply with all applicable Government regulations, policies and procedures (e.g., fire, safety, sanitation, environmental protection, security, "off limits" areas, wearing of parts of DHS uniforms, and possession of weapons) when visiting or working at Government facilities. The Contractor shall ensure Contractor employees present a professional appearance at all times and that their conduct shall not reflect discredit on the United States or the Department of Homeland Security. The Project Manager shall ensure Contractor employees understand and abide by Department of Homeland Security established rules, regulations and policies concerning safety and security.

8.5 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services required under the contract. The Contracting Officer shall provide the Contractor with a written explanation to support any request to remove an employee.

9.0 SPECIAL SECURITY REQUIREMENTS – CONTRACTOR Pre-Screening

Contractors requiring recurring access to Government facilities or access to sensitive but unclassified (SBU) information and/or logical access to Information Technology (IT) resources shall verify minimal fitness requirements for all persons/candidates designated for employment under any Department of Homeland Security (DHS) contract by prescreening the person/candidate prior to submitting their name for consideration to work on the contract. Pre-screening the candidate ensures that minimum fitness requirements are considered and mitigates the burden of DHS having to conduct background investigations on objectionable candidates. The Contractor shall submit only those candidates that have not had a felony conviction within the past 36 months, illegal drug use within the past 12 months, or misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months from the date of submission of their name as a candidate to perform work under this contract. Contractors are required to flow this requirement down to subcontractors. Pre-screening involves contractors and subcontractors reviewing. Felony convictions within the past 36 months. An acceptable means of obtaining information on felony convictions is from public records, free of charge, or from the National Crime Information Center (NCIC). Illegal

drug use within the past 12 months. An acceptable means of obtaining information related to drug use is through employee self-certification, by public records check; or if the Contractor or subcontractor already has drug testing in place. There is no requirement for contractors and/or subcontractors to initiate a drug testing program if they do not have one already in place. Misconduct such as criminal activity on the job relating to fraud or theft within the past 12 months. An acceptable means of obtaining information related to misconduct is through employee self-certification, by public records check, or other reference checks conducted in the normal course of business. Pre-screening shall be conducted within 15 business days after contract award. This requirement shall be placed in all subcontracts if the subcontractor requires routine physical access, access to sensitive but unclassified.

9.1 Suitability Determination/Entry on Duty Decision

Under the authority provided by Executive Order (EO) 13467, DHS requires that the Contractor workforce satisfy specific Contractor employee fitness requirements, similar to the suitability requirements as the federal workforce. DHS shall have and exercise full control over granting, denying, withholding, or terminating unescorted access to the government facility or sensitive government information access for Contractor employees, based upon the results of a background investigation. An entry on duty (EOD) is a favorable decision based on the Contractor completing all required forms and meeting eligibility requirement based on preliminary checks conducted by DHS to EOD as a Contractor.

9.2 **Continued Eligibility**

The Department of Homeland Security reserves the right and prerogative to deny and/or restrict access to the facility and information of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom DHS determines to present a risk of compromising sensitive government information to which the employee would have under this task order.

The Contractor shall immediately report any adverse information coming to their attention concerning contract employees under this task order to the COR. The Contractor must notify the Security Office of all terminations/resignations within two days of occurrence. The Contractor shall return any expired DHS issued identification cards and building passes, or those of terminated employees to the COR.

9.3 Access to DHS Facilities and Resources

DHS may exercise full control over granting, denying, withholding, or terminating unescorted access to DHS facilities, DHS systems, and/or sensitive DHS information for government/contract employees. Access shall be based upon the results of a DHS fitness/suitability investigation. DHS may, as appropriate, make favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the government/contract employee to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full DHS fitness/suitability authorization shall follow. The granting of a favorable EOD decision or a full DHS fitness/suitability authorization determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at

any time during the term of the contract/task order. No employee of the government / Contractor shall be allowed unescorted access to a DHS facility, access to any sensitive DHS information, or access to DHS Systems without a favorable EOD decision or DHS fitness/suitability determination by the DHS HQ Office of Security. Government/contract employees assigned to the contract/task order not needing access to sensitive DHS information, DHS systems, or access to DHS facilities shall not be subject to DHS fitness/suitability screening. Government/contract employees waiting on an EOD decision may not begin work on the task order. Limited access to DHS facilities is allowable prior to the EOD decision if the government/contract employee is escorted by an approved DHS employee. This limited access is to allow government/contract employees to attend briefings, nonrecurring meetings, and begin transition work. During one's limited access the government/contract employee shall not have access to sensitive or classified DHS information.

Classified information is government information which requires protection in accordance with Executive Order 13526, National Security Information (NSI) as amended and supplemental directives. If the government/contract employee has access to classified information at a DHS owned or leased facility, it shall comply with the security requirements of DHS and the facility. If the government/contract employee is required to have access to classified information at another Government Facility, it shall abide by the requirements set forth by the agency.

10.0 PERIOD OF PERFORMANCE

The period of performance for this contract is one base year and three optional one year periods from the date of award.

Base Period	09/05/2023 - 09/04/2024
Option Period 1:	09/05/2024 – 09/04/2025
Option Period 2:	09/05/2025 – 09/04/2026

10.1 PLACE OF PERFORMANCE

The on-site service shall be provided as required at the designated DHS locations within National Capital Region (NCR). The primary location of services is St. Elizabeth's campus but services may also be required at other DHS locations within the NCR. Requests shall be made by the PM, COR, or the employee receiving SLI services at a minimum of 24 hours prior to the assignment. Occasions may occur where the COR or alternate POC are unable to provide the required 24 hour notice. The Contractor shall have the right to refuse an assignment when less than 24 hour notice is given. The Contractor 's refusal must be given within two (2) hours of the time the request was placed during the business days. If the contractor accepts the request the agency shall be billed at the hourly rate established.

10.2 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 7:30 AM and 6:00 PM EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW.

10.3 TRANSITION OUT PLAN

The Contractor shall support the following transition-out activities to include the following:

- Provide a Transition-Out Plan no later than (NLT) ninety (90) days prior to the expiration of the task order period of performance (POP); the Transition-Out Plan shall be updated NLT thirty (30) days prior to the expiration of the POP: 08/02/2024
- Participate fully in all transition-out activities to the new Contractor to assume full responsibilities of the scope of the subsequent awarded task order,
- Continue to perform the duties in the SOW for the existing task order while transferring all documents, records, tickets, and deliverables to the new Contractor; and
- Ensure all government property included PIV / badges are returned to the COR or designated government personnel.

10.4 TRAVEL

The Contractor shall have the ability to travel with the DHS employee to local meetings, conferences, and trainings in a variety of locations within the National Capital Region (NCR).

Domestic travel may be required in connection with this contract. All domestic travel requires the advanced written approval of the COR. Travelers are required to submit a summary trip report to the COR within five working days following the completion of travel. Travel shall be in accordance with the Federal Travel Regulation. Local travel is defined as travel within 50 miles from the normal duty location. Local travel

shall not be reimbursed under this contract. Travel between Contractor personnel homes and the normal duty shall not be reimbursed under this contract.

Travel costs shall not be charged unless specifically authorized by order. In the event travel is approved, costs must follow GSA Joint Travel Regulations. No Contractor profit/fee or mark-ups (such as material handling fee) may be billed to the Government.

10.5 POST AWARD CONFERE NCE

The Contractor shall attend a Post Award Conference with the Contracting Officer (CO), Contract Specialist (CS), COR, and PM within 10 days after the date of award or as coordinated by the Contracting Officer. The Post Award Conference shall be held via teleconference. The date and time will be provided after award.

10.6 Quality Control Plan (QCP)

The Contractor must develop and maintain a Quality Control Plan (QCP) to be submitted and approved by the DHS BPA level CO which will outline what systems and activities the Contractor will implement to ensure that all services are provided in accordance with this PWS and the BPA. The QCP shall fulfill the following requirements:

- Establish an internal quality control, inspection and feedback system for all service required by orders.
- Provide the means to identify deficiencies in services and procedures to correct deficiencies and prevent recurrence. The QCP will include, but not be limited to, the following elements:
    - Methods to screen, evaluate, and train communications access specialists. The Contractor will explain how they will certify the proficiency of each specialist in English and the required sign language and CART services. The Contractor will explain how they will determine the minimum standards for the other services (audio description, Braille and reader services).The Contractor will explain how they will train communications access specialists in the procedures and terminology specific to the DHS operation or service.
    - Methods to track timeliness and performance with respect to established standards for responsiveness and quality of service. Methods to measure the effectiveness of the Contractor's quality control actions.

The QCP will also identify the individuals within the Contractor's organization with oversight authority over quality initiatives.

A draft version of the Quality Control Plan must be submitted with the Contractor quotation. The Contractor will provide a final version of the Plan for Government approval within 15 business days after BPA issuance and will continue to update and revise the Plan as needed throughout the life of the BPA. The Contractor will submit an ongoing monthly QC report that details actions taken, status and progress in implementing the QCP.

10.7 Quality Control Report

The report shall include a separate section for each Component and an overview for the Agency. The monthly quality control report shall include the Contractor 's methodology used to monitor the quality of the work under each order to ensure compliance with BPA and order requirements including the Performance Standards set forth in Table 3 of the PWS and order specific performance standards. The report shall include all incidents or services (identified either by the Contractor or the Government) which were considered to be non-conforming and the corrective action taken to correct performance to meet BPA and order requirements. The report shall include any changes made to the Contractors Quality Review Plan and its methodology to ensure continued compliance with the BPA and order requirements.

10.8 KICK-OFF MEETING

The Contractor shall attend a kick-off meeting for this task order as requested following award. The purpose of the kick-off meeting is to discuss technical objectives of the task order. The kickoff meeting, which shall be chaired by the COR, shall be held via teleconference. The date and time shall be provided after award by the COR or/and may be held concurrently with the Post Award Conference.

10.9 SECTION 508 COMPLIANCE

Pursuant to Section 508 of the Rehabilitation Act of 1973 (29 U.S.C. 794d) as amended by P.L. 105-220 under Title IV (Rehabilitation Act Amendments of 1998) all Electronic and Information Technology (EIT) developed, procured, maintained and/or used under this contract shall be in compliance with the "Electronic and Information Technology Accessibility Standards" set forth by the Architectural and Transportation Barriers Compliance Board (also referred to as the "Access Board") in 36 CFR Part 1194. The complete text of Section 508 Standards can be accessed at http://www.access-board.gov/ or at http://www.section508.gov.

11.0 GOVERNMENT TERMS & DEFINITIONS

- ASL – American Sign Language
- BPA – Blanket Purchase Agreement
- CART – Computer Aided Real-time Transcription
- COR – Contracting Officer's Representative
- CS – Contract Specialist
- CSC – Comprehensive Skills Certification
- DEIA - Diversity, Equity, Inclusion, & Accessibility
- DHS – Department of Homeland Security
- FSS – Federal Supply Schedule
- NCR – National Capital Region
- OES – Office of Enterprise Services
- PM – Program Manager
- PSE – Pidgin Signed English
- RID – Registry of Interpreters
- SLI – Sign Language Interpretation
- SEE – Signed Exact English
- S&T – Science & Technology

- VRI – Video Remote Interpreting

12.0 CONTRACT ADMINISTRATION DATA

12.1 CONTRACTING OFFICER / CONTRACT SPECIALIST

The Contracting Officer (CO) is:

Danette Williams
Office of Procurement Operations
Science & Technology Acquisition Division
Danette.Williams@hq.dhs.gov

12.2 CONTRACTING OFFICER'S AUTHORITY\

A warranted Contracting Officer is the only person authorized to issue modifications to the task order, approve changes in any of the requirements, or obligate funds. Notwithstanding any clause/provision contained elsewhere in this task order, the authority to modify the task order remains solely with the Contracting Officer. If the Contractor makes any task order changes at the direction of any person other than the Contracting Officer, the change shall be considered to have been made without authority and no adjustment shall be made in the task order to cover any increases in charges that may result. The Contracting Officer has the authority to perform any and all post-award functions in administering and enforcing the proposed task order in accordance with its terms and conditions.

12.3 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

The Contracting Officer may appoint a Contracting Officer's Representative (COR) to assist in monitoring the work under this task order. The COR is responsible for the technical administration of the task order and technical liaison with the Contractor. The COR IS NOT authorized to change the scope of work or specifications as stated in the task order, to make any commitments or otherwise obligate the Government or authorize any changes which affect the task order price, delivery schedule, period of performance, or other terms or conditions.

The COR for this task order is:

[redacted]

13.0 CONTRACT CLOSEOUT

In accordance with FAR 4.804, *Closeout of Contract Files*, the Contractor is required to participate in the closeout process. In addition, the contract closeout process shall be conducted at the end of the period of performance or termination of services, and upon receipt of evidence of physical completion of services and payment acknowledged by both the Contractor and Government.

14.0 INVOICE AND PAYMENT PROVISIONS

A. Invoices shall be prepared in accordance with FAR Clauses 52.212-4 Contract Terms and Conditions-Commercial Items Alternate I, incorporated into the Contractor's DHS BPA CAS, and BPA sections: B.21, *Billing Instructions*; and B.22, *Invoice Instructions*. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1. Cover sheet identifying DHS;
2. DUNS Number;
3. Task Order Number;
4. Modification Number, if any;
5. Month services provided; and
6. CLIN and Accounting Classifications.

B. The Contractor shall submit invoices monthly no later than the 10th calendar day of each month.

C. The Contractor shall indicate the associated CLIN, the number of hours dollar amount invoiced, fixed hourly rate, and service completed. All invoices shall include the current amount billed along with a cumulative amount billed and remaining balance. In addition, the invoice shall include the name of the ad hoc interpreter and the number of hours of services provided.

D. Also see "*REIMBURSEMENT FOR SERVICES- AD HOC INTERPRETER REQUESTS*"

E. The Assignment Log, Section 6.0, shall be submitted with the invoice.

F. **Distribution of invoices:** Invoices shall be sent via email to Invoice [redacted] identified on the task order with a copy electronically to the Contracting Officer's Representative (COR), and the Contracting Officer identified herein.

G. The Contractor shall prepare and submit a sufficient and procurement regulatory compliant invoice and receiving report for technical certification of inspection/acceptance of services and approval for payment. The Contractor shall attach back up information to the invoices and receiving reports substantiating all costs for services performed. The receiving agency's written or electronic acceptance by the COR and date of acceptance shall be included as part of the backup documentation. The Government reserves the right to have all invoices and backup documentation reviewed by the Contracting Officer prior to payment approval. If the invoice is submitted without all required back up documentation, the invoice shall be rejected.

Revised/Replaced Rejected Invoice: The revised invoice to replace rejected invoice shall have the same number as the rejected invoice with an "R" added at the end of the invoice number to identify that the invoice has been revised/corrected.

15.0 SPECIAL CONTRACT REQUIREMENTS

14.1 SECURITY REQUIREMENTS

15.1.1 Suitability Determination/Entry on Duty Decision

Under the authority provided by Executive Order (EO) 13467, DHS requires that the Contractor workforce satisfy specific Contractor employee fitness requirements, similar to the suitability requirements as the federal workforce. DHS shall have and exercise full control over granting, denying, withholding, or terminating unescorted access to the government facility or sensitive government information access for Contractor employees, based upon the results of a background investigation. An entry on duty (EOD) is a favorable decision based on the Contractor completing all required forms and meeting eligibility requirement based on preliminary checks conducted by DHS to EOD as a Contractor.

15.1.2. Continued Eligibility

The Department of Homeland Security reserves the right and prerogative to deny and/or restrict access to the facility and information of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom DHS determines to present a risk of compromising sensitive government information to which the employee would have under this task order.

The Contractor shall immediately report any adverse information coming to their attention concerning contract employees under this task order to the COR.

The Contractor must notify the Security Office of all terminations/resignations within two days of occurrence. The Contractor shall return any expired DHS issued identification cards and building passes, or those of terminated employees to the COR.

15.1.3 Employee Identification/Building Pass

In accordance with DHS' security policy, *"Post Award Instructions Regarding Security Requirements for Non-Classified Contracts/Orders"*, provided in Section 4.4 below, the Contractor shall coordinate with the COR to assure that any Contractor employee requiring access to the DHS offices has a Contractor identification/building pass before the employee enters on duty. Personnel designated by the COR shall complete appropriate forms specified by the DHS Office of the Chief Security Officer for security clearance requirements.

Contractor employees working on-site at Government facilities shall wear a Government issued identification badge at all times. All Contractor employees shall identify themselves as Contractors when their status is not readily apparent (in meetings, when answering Government telephones, in e-mail messages, etc.) and display the Government issued badge in plain view above the waist at all times.

Contractor employees visiting Government facilities shall wear an identification badge that, at a minimum, displays the Contractor name, the employee's photo, name, clearance-level and badge expiration date. Visiting Contractor employees shall comply with all Government escort rules and requirements.

All Contractor employees shall identify themselves as Contractors when their status is not

readily apparent and always display all identification and visitor badges in plain view above the waist.

The Contractor shall see that all passes are returned to the Government as employees are dismissed, terminated or when the need for the employee to have access to DHS offices ceases.

15.2 Post Award Instructions Regarding Security Requirements for Non-Classified Contracts/Orders

1. The procedures outlined below shall be followed for the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD) to process background investigations, Entry on Duty determinations, and Fitness determinations, as required, in a timely and efficient manner.
2. Carefully read the security clauses in the contract. Compliance with the security clauses in the contract is not optional.

3. 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 shall perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations shall be processed through the DHS OCSO/PSD. Prospective Contractor employees shall submit the below completed forms to the DHS forms to the DHS OCSO/PSD. The Standard Form (SF) 85-P must be completed electronically through the Office of Personnel Management's e-QIP SYSTEM. The SF-85P signature pages and other completed forms must be given to the OSCO/PSD no less than thirty (30) days before the start date of the contract or thirty (30) days prior to the requested entry on duty date, for all Contractor employees whether a replacement, addition, subcontractor employee, or vendor:

   e. Standard Form (SF) 85-P, "Questionnaire for Public Trust Positions"

   iii. SF-85P Certification
   iv. SF-85P Authorization for Release of Medical Information

   f. FD Form 258, "Fingerprint Card" (2 copies)
   g. DHS Form 11000-6, "Conditional Access to Sensitive but Unclassified Information Non-Disclosure Agreement"
   h. DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act" Only complete packages shall be accepted by the DHS OCSO/PSD. Specific instructions on submission of packages shall be provided upon award of the contract.

4. 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 shall 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 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. The intent of this statement is to allow a minimum amount of meeting / transition attendances to prepare for the new contract.

5. 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.

6. In accordance with DHS HSAR 3052.204-71, 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 or not 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).

7. Your point of contact (POC) at the Security Office is:
   DHS OCSO/PSD Security Customer Service Center
   E-mailbox: [redacted]

15.3 Disclosure of Information

a. Contractors are reminded that information furnished under this solicitation 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 shall not necessarily preclude disclosure when the U.S. Office of Personnel Management (OPM) or the Government determines disclosure is warranted by FOIA. However, if such items are not marked, all information contained within the submitted documents shall be deemed to be releasable.

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

c. In performance of this task order, 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.

d. 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 19 U.S.C. 641, *Public Money, Property or Records*. That section provides, in pertinent part, that whoever knowingly converts to their use or the use of another, or without authority, sells, conveys, or disposes of any record of the United States or whoever receives the same with intent to convert it to their use or gain, knowingly it to have been converted, shall be guilty of a crime punishable by a fine of up to $10,000, or imprisoned up to ten years, or both.

10.1 **DELIVERABLES**

The Contractor shall consider items in **BOLD** as having mandatory due dates. Items in *italics* are deliverables or events that must be reviewed and/or approved by the COR prior to proceeding to next deliverable or event in this SOW.

ASSIGNMENT LOG

The Contractor shall maintain a log of the dates an order was placed, the time the order was placed, the job number, the date of the assignment, the start time of the assignment, the anticipated duration and a description of the event for each assignment given to the Sign Language Interpreters. The log shall be made available to the COR as requested for inspection; however, the final assignment log shall be submitted with the invoice by the 10th of each month.

ITEM	SOW REFERENCE	DELIVERABLE / EVENT	DUE BY	DISTRIBUTION
1	10.5	Post Award Conference	Within 10 days after award or as coordinated by CO.	COR, Contracting Officer
2	10.6	*QCP*	Within 15 days after BPA issuance	COR, Contracting Officer
3	10.7	*Quality Control Report*	Monthly	COR, Contracting Officer
2	10.8	*Kick-Off Meeting*	No later than 15 days after the date of award.	COR, Contracting Officer
3	6.0	*Assignment Log*	10th of each month	COR, Contracting Officer

Organization Conflict of Interest/Task Order Specific Clauses

Organizational Conflict of Interest Notice

(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:

(1) Potential offerors may have had access to non-public Government information that would provide an unfair competitive advantage under the present solicitation,

(2) Potential offerors may have an unfair competitive advantage because they developed or established the ground rules for the present solicitation, or

(3) Potential offerors may have an unfair competitive advantage because they have been in a position to evaluate other potential competitors or they had access to the non-public information of other potential competitors under this solicitation.

(4) Potential offerors have a conflicting role that will prevent them from providing unbiased advice or assistance.

(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:
X (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 quote, 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.

3052.209-73 Limitation of Future Contracting.

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.

(b) The nature of this conflict is

(1) The Contractor may gain access to non-public Government information that would provide an unfair competitive advantage under a future acquisition,

(2) The Contractor may gain an unfair competitive advantage because it developed or established the ground rules for a future acquisition, or,

(3) The Contractor may gain an unfair competitive advantage because it will be placed in a position to evaluate potential competitors or gain access to the non-public information of other potential competitors under a future acquisition.

(c) 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*)

FAR Clauses Incorporated by Full Text

The following FAR Clauses are hereby incorporated in full text to this Contract:

FAR 52.204-27 Prohibition on a ByteDance Covered Application (Jun 2023)

(a) Definitions. As used in this clause—

Covered application means the social networking service TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited.

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

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

(i) Of that equipment; or

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

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

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

(b) Prohibition. Section 102 of Division R of the Consolidated Appropriations Act, 2023 (Pub. L. 117-328), the No TikTok on Government Devices Act, and its implementing guidance under Office of Management and Budget (OMB) Memorandum M-23-13, dated February 27, 2023, "No TikTok on Government Devices" Implementation Guidance, collectively prohibit the presence or use of a covered application on executive agency information technology, including certain equipment used by Federal contractors. The Contractor is prohibited from having or using a covered application on any information technology owned or managed by the Government, or on any information technology used or provided by the Contractor under this contract, including equipment provided by the Contractor's employees; however, this prohibition does not apply if the Contracting Officer

provides written notification to the Contractor that an exception has been granted in accordance with OMB Memorandum M-23-13.

(c) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts, including subcontracts for the acquisition of commercial products or commercial services.

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 15 days of the period of contract expiration.
(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 15 days of contract expiration provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 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 36 months.
(End of clause)

FAR 52.222-40 Notification of Employee Rights Under the National Labor Relations Act (Dec 2010)

(a) During the term of this contract, the Contractor shall post an employee notice, of such size and in such form, and containing such content as prescribed by the Secretary of Labor, in conspicuous places in and about its plants and offices where employees covered by the National Labor Relations Act engage in activities relating to the performance of the contract, including all places where notices to employees are customarily posted both physically and electronically, in the languages employees speak, in accordance with 29 CFR 471.2 (d) and (f).
(1) Physical posting of the employee notice shall be in conspicuous places in and about the Contractor's plantsand offices so that the notice is prominent and readily seen by

employees who are covered by the National Labor Relations Act and engage in activities related to the performance of the contract.

(2) If the Contractor customarily posts notices to employees electronically, then the Contractor shall also post the required notice electronically by displaying prominently, on any website that is maintained by the Contractor and is customarily used for notices to employees about terms and conditions of employment, a link to the Department of Labor's website that contains the full text of the poster. The link to the Department's website, as referenced in (b)(3) of this section, must read, "Important Notice about Employee Rights to Organize and Bargain Collectively with Their Employers."

(b) This required employee notice, printed by the Department of Labor, may be:

(1) Obtained from the Division of Interpretations and Standards, Office of Labor-Management Standards, U.S. Department of Labor, 200 Constitution Avenue, NW., Room N-5609, Washington, DC 20210, (202) 693-0123, or from any field office of the Office of Labor–Management Standards or Office of Federal Contract Compliance Programs;

(2) Provided by the Federal contracting agency if requested;

(3) Downloaded from the Office of Labor–Management Standards Web site at http://www.dol.gov/olms/regs/compliance/EO13496.htm; or

(4) Reproduced and used as exact duplicate copies of the Department of Labor's officialposter.

(c) The required text of the employee notice referred to in this clause is located at Appendix A, Subpart A, 29 CFRPart471.

(d) The Contractor shall comply with all provisions of the employee notice and related rules, regulations, and orders of the Secretary of Labor.

(e) In the event that the Contractor does not comply with the requirements set forth in paragraphs (a) through (d) of this clause, this contract may be terminated or suspended in whole or in part, and the Contractor may be suspended or debarred in accordance with 29 CFR 471.14 and subpart 9.4. Such other sanctions or remedies may be imposed as are provided by 29 CFR part 471, which implements Executive Order 13496 or as otherwise provided by law.

(f) Subcontracts.

(1) The Contractor shall include the substance of this clause, including this paragraph (f), in every subcontract that exceeds $10,000 and will be performed wholly or partially in the United States, unless exempted by the rules, regulations, or orders of the Secretary of Labor issued pursuant to section 3 of Executive Order 13496 of January 30, 2009, so that such provisions will be binding upon each subcontractor.

(2) The Contractor shall not procure supplies or services in a way designed to avoid the applicability ofExecutive Order 13496 or this clause.

(3) The Contractor shall take such action with respect to any such subcontract as may be directed by the Secretary of Labor as a means of enforcing such provisions, including the imposition of sanctions for noncompliance.

(4) However, if the Contractor becomes involved in litigation with a subcontractor, or is threatened with such involvement, as a result of such direction, the Contractor may

request the United States, through the Secretary of Labor, to enter into such litigation to protect the interests of the United States.

(End of clause)

FAR 52.224-3 Privacy Training – Alternate I (DEVIATION)

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

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

(1) Have access to a system of records;

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

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

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

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

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

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

(1) Have access to a system of records;

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

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

(End of clause)

U. S. Department of Homeland Security Acquisition Regulation (HSAR Clauses Incorporated by Full Text)

The full text of the **Homeland Security Acquisition Regulation (HSAR)** may be accessed electronically at: http://www.dhs.gov/xlibrary/assets/opnbiz/hsar.pdf. The following HSAR Clauses are hereby incorporated in Full Text:

Notwithstanding the following, it is not the Government's intention to share with Contractor any "Sensitive Information" as defined in 48 C.F.R 3052.204-71(a) or information deemed "sensitive" as used in 48 C.F.R 3052.204-71(a)(4) such that the Government would require access be limited to only citizens of the United States of America or lawfully admitted aliens. In the event the Government needs to share "Sensitive Information" or information deemed "sensitive" as used in 48 C.F.R 3052.204-71, in subsequent task orders, the Government will identify the information for which the restriction applies to the Contractor in the given task order.

If any contractors need access to "sensitive" information, access to DHS IT equipment or need unescorted access in DHS facilities submission for DHS Contractor Fitness will be required.

Before any foreign nationals start working on this contract they must be submitted for vetting and cleared by DHS S&T Security prior to beginning work.

HSAR 3052.204-71 Contractor Employee Access (JUL 2023) Alternate II (JUL 2023)

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 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 3052.205-70 Advertisements, Publicizing Awards, and Releases (Sep 2012)

The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

(End of clause)

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

***(a)* Prohibitions.**

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) **Definitions**. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the

Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

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

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

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;
(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held—
(3) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or (ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and
(4) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.
(5) *Person, domestic, and foreign* have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.
(6) **Special rules**. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.
(7) *Certain stock disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:
(8) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or
(9) Stock of such entity which is sold in a public offering related to an acquisition described in section 835(b)(1) of the Homeland Security

Act, 6 U.S.C. 395(b)(1).

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

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

(12) **Special rule for related partnerships**. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(13) **Treatment of Certain Rights**.

(14) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows: (i) warrants;

(15) options;

(16) contracts to acquire stock; (iv) convertible debt instruments; and (v) others similar interests.

(17) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(18) **Disclosure**. The offeror under this solicitation represents that [Check one]:

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

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

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

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

(End of clause)

HSAR 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 under this Contract: (tbd)

SAFEGUARDING OF CONTROLLED UNCLASSIFIED INFORMATION (JULY 2023)

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

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

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

(1) Chemical-terrorism Vulnerability Information (CVI) as defined in 6 CFR part 27,

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

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

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

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

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

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

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

(i) Department of Homeland Security information technology (IT) systems data revealing

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

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

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

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

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

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

(i) Examples of stand-alone PII that are particularly sensitive include: Social Security numbers (SSNs), driver's license or State identification numbers, Alien Registration

Numbers (A-numbers), financial account numbers, and biometric identifiers.

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

(A) Truncated SSN (such as last 4 digits);
(B) Date of birth (month, day, and year);
(C) Citizenship or immigration status;
(D) Ethnic or religious affiliation;
(E) Sexual orientation;
(F) Criminal history;
(G) Medical information; and
(H) System authentication information, such as mother's birth name, account passwords, or personal identification numbers (PINs).

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

Federal information means information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.
Federal information system means an information system used or operated by an agency or by a Contractor of an agency or by another organization on behalf of an agency.

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

Incident means an occurrence that—

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

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

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

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

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

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

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

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

(b) *Handling of Controlled Unclassified Information.*

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

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

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

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

(c) *Incident Reporting Requirements.*

(1) Contractors and subcontractors shall report all known or suspected incidents to the

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

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

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

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

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

(i) Unique Entity Identifier (UEI);
(ii) Contract numbers affected unless all contracts by the company are affected;
(iii) Facility CAGE code if the location of the event is different than the prime Contractor

location;
(iv) Point of contact (POC) if different than the POC recorded in the System for Award Management (address, position, telephone, and email);
(v) Contracting Officer POC (address, telephone, and email);
(vi) Contract clearance level;
(vii) Name of subcontractor and CAGE code if this was an incident on a subcontractor network;
(viii) Government programs, platforms, or systems involved;
(ix) Location(s) of incident;
(x) Date and time the incident was discovered;
(xi) Server names where CUI resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the government PII or SPII contained within the system; and
(xiii) Any additional information relevant to the incident.

(d) *Incident Response Requirements.*

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

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

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

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

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

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

(e) *Certificate of Sanitization of Government and Government-Activity-Related Files and*

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

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

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

(End of Clause)
