# STATEMENT OF WORK

## Department of Homeland Security (DHS)
## Office of Immigration Detention Ombudsman (OIDO)

## 1.0 GENERAL

### 1.1 Background

The Office of the Immigration Detention Ombudsman (OIDO) was established by Congress on December 20, 2019, per Sec. 106 of the Consolidated Appropriations Act, 2020, Public Law 116-93. OIDO acts as an independent office within the Department of Homeland Security (DHS) to resolve problems related to the detention of individuals and families, as mandated under current immigration law.

To fulfill the DHS mandate in all aspects, OIDO requires access to a comprehensive set of high-quality language services for interactions with individuals and families whom OIDO encounters at detention facilities. This must include a full array of language services to ensure effective communication with persons who are non or limited English speaking that support OIDO in carrying out its independent oversight mission in compliance with federal law.

### 1.2. Scope

The Statement of Work (SOW) covers Foreign Language Services. Services requested include translation, interpretation (on-site, telephonic), and transcription. The purpose of this SOW is to obtain high quality timely services to carry out the OIDO mission ensuring meaningful access to Limited English Proficient (LEP) persons to resolve problems related to the detention of individuals and families.

## 2.0 REQUIREMENTS

**2.1** The Contractor shall provide language services through qualified linguists as specified in the DHS Language Services II strategic sourcing vehicle. The Language Services II BPA provides Foreign Language Services for approximately 180 languages and dialects.

**2.2** OIDO requires language services for anticipated and/or routine interactions as well as language services that support emergency situations. Therefore, the Contractor shall have the capacity to meet higher demands and fulfill critical and time-sensitive language needs.

**2.3** For both routine and unexpected situations, the Contractor must be able to provide support 24 hours a day, 7 days a week, 365 days per year (inclusive of weekends and holidays) for all categories of language services described herein.

**2.4** The Contractor shall furnish the necessary labor personnel and materials (equipment, travel, and ancillary labor) required to satisfy the BPA call requirements. Language Service may be required at any location within the United States and its territories. The Contractor shall supply qualified language specialists to work on-site at the locations required from local sources when possible. Cost associated with local travelshall not be charged to OIDO.

**2.5** The contractor must have rigorous quality control processes for all language services provided as detailed within the SOW. These quality control reports must be made available to the Program Office for review and verification at any time upon request.

**2.6** The Contractor shall have the capability of telecommunication technology (i.e., landline, cell phone, video communication (e.g., Microsoft Teams, Zoom), email, fax, and basic internet function) to provide services.

**2.7** The Contractor shall provide and maintain a secure, web-based interface/portal which allows access to task order performance data at all times as set forth in the DHS BPA PWS. The portal shall be available to the OIDO COR to conveniently generate reports, analysis, and other self-produced ad-hoc queries. Performance data shall be maintained in a manner which allows self-generated reports to be exportable in Microsoft Excel format. Real-time reports may have up to a 1-hour lag time.

## 3.0 LANGUAGE SERVICES REQUIRED

In order to fulfill OIDO's mission, we require routine access to a full range of language services delivered in a variety of contexts. The contractor shall be prepared to serve LEP persons in languages "requested most often" listed in Appendices A and B of the SOW. The Contractor shall provide languages not identified as "requested most often" listed in Appendices A and B on a best effort basis.

Department of Homeland Security (DHS) Language Services II BPA includes foreign language interpretation, translation, and transcription services. The Office of Immigration Detention Ombudsman (OIDO) is seeking a task order in support of work performed on-site at any location OIDO personnel or contract staff are located within the continental United States and its territories.

OIDO has a need to meet its current requirement through a language line service for Program Office and contract staff that provides accessibility 24/7/365. The language line established by the Contractor shall be equipped to provide language services for most frequently requested

languages and less common languages, on an on-demand basis.

OIDO requires these services to be delivered in diverse contexts with the skills and knowledge as set forth herein.

The Contractor shall furnish all personnel, supervision, equipment, materials, transportation, and other items necessary to perform the services described in the SOW.

A detailed description of the work required, any specialized personnel skillsets, and the place of performance will be set forth within the SOW.

OIDO and contract staff are authorized to request language services under the task order so they can fulfill their official agency duties without delay.

**4.0 SPECIFIC REQUIREMENTS/TASKS**

a. The Contractor shall meet all task order requirements by providing linguists who meet the personnel qualifications set forth in Section 7 of this SOW and Section 4 of the DHS Language Services BPA PWS and Appendix D there within.

b. The Contractor shall establish a custom, direct phone line dedicated to OIDO personnel.

c. OIDO requires language services for anticipated and/or routine interactions as well as language services that support surges and emergency situations. Therefore, the Contractor shall have the ability and capacity to rapidly increase its staffing level for any given language in an expedited manner to meet time sensitive OIDO language needs.

d. For both routine and unexpected situations, the Contractor must be able to provide support 24 hours a day, 7 days a week, 365 days per year (inclusive of weekends and holidays) for all categories of language services described herein. Upon award, the selected Contractor must provide at least two designated points of contact (POC). At least one POC shall be able to answer finance, funding, or billing related questions and one shall be able to answer service-related matters such as: the progress and status of linguist clearances, quality assurance, staffing questions, and the production of reports.

e. POCs shall be available during normal business hours, 9 a.m. – 5 p.m. ET (business hours can be lenient if a Contractor is in another time zone). The Contractor shall provide POCs who have the authority to make decisions,or who can obtain them easily, but who are also familiar with the contract requirements and OIDO needs.

f. The Contractor shall demonstrate how to ensure that all linguists who will perform work under this task order meet the minimum personnel qualification requirements as outlined in this task order. The Contractor shall also include a contingency plan for replacing or substituting linguists when those originally assigned to the task order are not able to perform or meet the task order requirements.

g. The Contractor shall provide and maintain a secure, web-based interface/portal which allows access to task order performance data, broken out by each Division within OIDO and other criteria specific within the task order, at all times. The portal shall be available to the COR and OIDO officials to generate reports or conduct self-produced ad-hoc queries or analysis. Performance data shall be maintained in a manner which allows self-generated reports to be exportable in a Microsoft Excel format. Real-time reports may have up to a 1-hour lag time and available information should include:

- Cumulative task order-to-date activity, year-to-date activity, month-to-date activity, and daily activity [by OIDO Division, language, service type and cost].
- Detailed itemization of each contact shall be recorded and be available upon request (a contact is defined as successful communication using any form of language services within the scope of the OIDO task order).
    - Contact data shall include the following:
        - Date and time of contact
        - Requesting OIDO employee (federal) or contractor's name and PIN
        - Requesting employee's division
        - Language that was interpreted/translated/transcribed
        - Telephone Interpreter call request: date, start, end, total minutes, and total duration

## 5.0 LANGUAGE SERVICES REQUIRED

As stated under Section 2.1(a) of the DHS Language Services PWS, the general requirements of FC1 include language services as defined under GSA Schedule 738II Language Services - Translation Services (381-1) and Interpretation Services (382-2). The Contractor must have the ability to provide all of the services listed in this SOW.

## 5.1 FOREIGN LANGUAGE INTERPRETATION

OIDO requires telephonic interpretation and periodic on-site oral communication to and from English and foreign languages in a variety of settings, including, but not limited to: intake screening and processing of detainees, interviews, interpreting of detainee grievances, communicating processes and responsibilities, presentations and discussions that may include conversations between OIDO personnel and individuals detained, witnesses, victims, and other external stakeholders.

The Contractor shall provide foreign language interpretation by interpreting oral communication to and from English and foreign languages telephonically, video communication, or in-person. Interpretation includes but is not limited to: simultaneous, consecutive, sight translation, telephonic and voiceovers. Interpreter forums may include meetings, conferences, briefings, and training.

The Contractor shall provide interpretation services in all languages indicated in Appendix B,

as well as other languages or dialects not yet encountered by OIDO on an as needed and on a best effort basis.

The Contractor shall have the ability to telephonically assist OIDO employees and contract staff in the identification of a Limited English Proficient (LEP) individual's primary language, when encountered. There may be instances in which an individual encountered may be illiterate or not speak one of the languages listed. In the Contractor's response to this task order, the Contractor shall communicate how it plans to perform the responsibility to identify a LEP individual's primary language, as needed.

Telephonic Interpretation: The Contractor shall provide interpreters telephonically to support calls placed by OIDO personnel, contract staff, or facilities that need to communicate with ICE or CBP detainees. Language interpretation services is based on the volume of detainee complaints filed with OIDO to investigate and resolve. Therefore, it is impossible to know exactly how many hours' worth of calls the Contractor will receive in any given period of time. Therefore, OIDO does not guarantee a minimum amount of call volume the Contractor will incur, nor can it predict which months, days, or time of day will be the busiest.

- The Contractor shall provide telephonic interpretation 24 hours per day, 7 days per week, and 365 days per year.

- The Contractor shall provide on-site interpretation within a reasonable timeframe, if requested by an OIDO employee or OIDO contract staff employee.

- The Contractor shall provide toll free prompt access to skilled linguists.

- When taking calls, linguists must be located within the continental United States and its territories (i.e., Puerto Rico, Guam, etc.). Although it is not a qualifying factor, the Contractor shall notify OIDO in their response to this task order if they have the ability to record calls should a situation arise in which it is requested.

- If the language requested by an OIDO employee or contractor is not available immediately upon call, an estimated time for locating the appropriate interpreter must be provided. Interpretation shall be provided within the timeframes outlined in table SSPA-4. If a request cannot be fulfilled for any reason, a designated vendor POC shall notify the OIDO task order COR or the Contracting Officer immediately so appropriate arrangements can be made to assist the requesting office in obtaining the necessary language services.

- Each linguist shall identify themselves before initiating interpretation by a unique code that the Contractor has assigned to maintain confidentiality.

- The Contractor must have a back-up plan in place to address any malfunction of its technical systems used to support telephonic interpretation without interruption.

- The Government will not be charged for calls made unless a call is placed the

vendor that results in the actual use of interpretation services. The Government shall not be charged for calls scheduled then cancelled by OIDO staff, calls abandoned by the interpreter, instances when confidentiality is violated or when an interpreter is recused for bias, when connectivity is lost, and when the interpreter does not demonstrate required fluency.

Performance will be evaluated to determine whether or not it meets the requirements of the task order. When the COR advises the Contracting Officer that Contractor performance is problematic, the Contracting Officer may deem it appropriate to issue a Contract Discrepancy Report.

## 5.2 FOREIGN LANGUAGE TRANSLATION

OIDO requires translation of many kinds of written documents, including, but not limited to: policies, forms, handbooks, audio recordings, flyers, posters, and reports. The Contractor shall provide translation services in a timely manner in all languages indicated in Appendix A as well as obtain other languages or dialects encountered on an as needed basis and on best effort basis.

The Contractor shall provide translation by translating written, electronic and/or multi-media material to and from English and foreign languages. Materials include but are not limited to: legal, medical, policy, video subtitling, audio recordings, and captioning. Translation includes formatting, proofreading, text adaptation, editing, graphic design, and desktop publishing. Specialized certifications or knowledge base may be required (e.g., medical or court certified) as needed.

Translation shall be provided within the timeframes outlined in table SSPA-5. If a translation request cannot be fulfilled for any reason, including pending clearance requirements, a designated Contractor POC shall notify the OIDO task order COR or Contracting Officer immediately so appropriate arrangements can be made to assist the requesting office in obtaining the necessary language services.

Each translation is to be a complete, precise, and idiomatically correct rendering from the source language into the target language. The translation is to be reviewed and certified by the Contractor as a true and accurate translation of the document as admissible in court or meet the needs of the target audience when the document is not intended to be submitted to a court. A Translation Certification Form should be provided with each translation; the individual certifying the translation shall be a person other than the original translator and fluent in both the target language being certified and English.

## 5.3 FOREIGN LANGUAGE TRANSCRIPTION/CAPTIONING SERVICES

OIDO requires transcription services of converting speech from audio/video sources or other formats into a written or electronic text document to and from English and foreign languages. The Contractor shall provide services in all languages indicated in Appendix A as well as be able to obtain linguists in a timely manner for other languages or dialects encountered on an as needed basis and on a best effort basis.

The Contractor shall provide foreign language transcription by interpreting oral communication (live or recorded) to and from English and foreign languages and transcribing it into written, electronic and/or multi-media material/format showing verbatim words from the conversation or the recording. End product is stored on a removable media with a printed copy or provided electronically, depending on agency personnel preference. Materials include but are not limited to legal, medical, policy, video subtitling, audio recordings and captioning. Transcription includes formatting, proofreading, text adaptation, editing, graphic design, and desktop publishing. Specialized certifications or knowledge base (e.g. medical or court certified) may be required as needed.

Each transcription is to be a complete, precise, and idiomatically correct rendering from the source into the target language and is to be reviewed and certified by the Contractor as a true and accurate translation of the document as admissible in court or to meet the needs of the target audience when the document is not intended to be submitted to a court. A Transcription Certification Form should be provided with each transcription; the individual certifying the transcription shall be a person other than the original translator and fluent in both the target language being certified and English.

## 6.0 CONTRACTOR PERSONNEL

The Contractor shall provide all necessary personnel to meet task order requirements and provide effective management of the task order, including but not limited to: program/project management, human resource management, performance management, quality assurance, administrative support, and supervision of all Contractor staff. Contractor supervisors shall perform proper oversight of all Contractor employees. Contractor supervisor(s) shall perform supervisory/management activities to ensure that Contractor employees have necessary skills, information, and tools to perform tasks and that task order requirements are properly met. All Contractor employees shall address personnel and program issues through their supervisors and not directly through OIDO's management personnel.

## 7.0 LANGAUGE SPECIALIST PERSONNEL QUALIFICATIONS

All Contractor personnel providing services under this task order shall meet the minimum qualifications and proficiency levels set forth in Appendix A attached of the DHS Language Services II BPA under Tier 2, Minimum Requirements.

## 8.0 QUALITY CONTROL

The Contractor shall be solely responsible for the quality of services provided.

The Contractor must develop and maintain a Quality Control Plan (QCP) to be submitted and approved by the OIDO task order Contracting Officer (CO) who will outline what systems and activities the Contractor will implement to ensure that all services are provided in accordance with this SOW and the BPA. The QCP shall fulfill the following requirements:

- Establish an internal quality control, inspection and feedback system for all services required by task 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 test, train, evaluate, and certify language specialists. The Contractor will explain how it will certify the proficiency of each language specialist in English and the required language. The Contractor will explain how it will train language 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.

The Contractor will provide a final version of the QCP within 15 business days after task order award and will continue to update and revise the Plan as needed throughout the life of the task order and option years. The Contractor will submit an ongoing monthly QC report that details actions taken, status and progress in implementing the QCP. See Section 15, Reporting Requirements.

The DHS Contracting Officer, in writing, may require that the Contractor remove and replace any Contractor employee that: a) is not fluent in the language(s) requested, b) fails to adhere to DHS or Component standards of conduct or any Recognized industry standards, or c) fails to meet BPA or task order security requirements. Corrective action may be taken to resolve and remedy situations involving any removed employees after notification details have been sent to the OIDO COR and CO in accordance with procedures of a QCP of the Contractor.

The Contractor shall certify each translation and transcription and return a certification electronically with the completed request. The technical and linguistic accuracy of each translation and transcription is of paramount importance to the Government. Each translation and transcription is to be a complete, precise, and idiomatically correct rendering from the source language into the target language and is to be reviewed and certified by the Contractor as a true and accurate translation of the document as admissible in court or meet the needs of the target audience when the document is not intended to be submitted to a court. The individual certifying the translation/transcription shall be a person other than the original translator and fluent in both the target language being certified and English. The project will not be considered complete until the certification is received.

## 9.0 CONFIDENTIALITY AND PRIVACY CONSIDERATIONS

a. Non-Disclosure Agreements are required to be signed by all Contractor personnel when their role requires them to come into contact with Sensitive but Unclassified, Government procurement sensitive information, and/or other sensitive information, or

proprietary business information from other Contractors. The Contracting Officer will provide the prescribed non-disclosure forms as necessary to the Contractor when circumstances warrant. The Contractor shall maintain, transmit, retain in the strictest confidence, and prevent the unauthorized duplication, use, and disclosure of information.

b. When applicable, the Contractor shall provide information only to Homeland Security Presidential Directive 12 (HSPD-12) cleared employees, contractors, and subcontractors having a "need-to-know" of such information in the performance of their duties for this project.

c. The recipient of information certifies in writing that he or she will take the necessary steps to prevent the unauthorized disclosure and use of information. The CO shall provide the prescribed non-disclosure agreement forms as necessary to the Contractor.

- Information made available to the Contractor by the Government for the performance or administration of this effort shall be used only for those purposes and shall not be used in any other way without the written agreement of the Component CO.

- The Contractor agrees to assume responsibility for protecting the confidentiality of Government records that are not public information. Each employee or subcontractor of the Contractor to whom information may be made available or disclosed shall use the information provided only for a purpose and to the extent authorized herein. Penalties for non-approved release of privacy data shall be subject to penalties described in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a.

- Performance of this effort may require the Contractor to access and use data and information proprietary to a Government Component or Government Contractor which is of such a nature that its dissemination or use, other than in performance of this effort, would be adverse to the interests of the Government and/or others.

- The Contractor and its personnel shall not divulge or release data or information developed or obtained in performance of this effort, until made public by the Government, except to the authorized Government personnel or upon written approval of the Contracting Officer. The Contractor shall not use, disclose, or reproduce proprietary data that bears a restrictive legend, other than as required in the performance of this effort.

- All deliverables, source code, reports, audio productions, and data received, processed, evaluated, loaded, and/or created as a result of this task order shall remain the sole property of the Government unless specific exception is granted in writing by the task order CO.

- The Contractor and its personnel/employees shall NOT keep any personally identifiable information (PII) obtained through language services performed under this task order. The Contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally

identifiable information (as defined by the Office of Management and Budget [OMB]) was, or is reasonably believed to have been, breached. Any notification shall be coordinated with DHS and shall not proceed until DHS decides that notification would not impede or jeopardize national security. The method and content of any notification by the Contractor shall be coordinated with and be subject to the approval of DHS. The Contractor assumes full responsibility for taking corrective action, which may include offering credit monitoring, when appropriate.

## 10. SECURITY REQUIREMENTS

## CONTRACTOR PERSONNEL

### Qualified Personnel

The Contractor shall provide qualified personnel to perform all requirements specified in this SOW.

### 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 is designated as key for this requirement: **Project Manager**

### Replacement of Key Personnel

Before replacing any individual designated as Key by the Government, the Contractor must 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 must possess qualifications equal to or superior to those of the Key person being replaced. The Contractor must not replace Key Contractor personnel without acknowledgment from the Contracting Officer.

### 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 will not be provided, the Contractor shall provide e-mail notification to the Contracting Officer's Representative (COR) prior to employee absence. Otherwise, the Contractor shall provide a fully qualified replacement.

### Employee Identification

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.

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.

**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.

**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 will provide the Contractor with a written explanation to support any request to remove an employee.

**OTHER APPLICABLE CONDITIONS**

**SECURITY**

Contractor access to unclassified, but Security Sensitive Information may be required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination.

**Requests for Exception to U.S. Citizenship Requirement**

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to citizenship requirements are treated differently from security policy waivers. Exceptions to the U.S. citizenship requirement should be requested by completing a Foreign National Visitor Access Request, DHS Form 11052-1, which is available online or through the DHS Office of the Chief Security Officer (OCSO). Components who have access may file their request via the Foreign National Vetting Management System (FNVMS), a part of the DHS OCSO Integrated Security Management System's (ISMS). For further information regarding the citizenship exception process, contact the DHS OCSO

This Policy Directive and the DHS 4300A, Information Technology System Security Program, Sensitive Systems apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS information unless an approved waiver has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).

**POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS**

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

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

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

  - Standard Form 85P, "Questionnaire for Public Trust Positions"
  - FD Form 258, "Fingerprint Card" (2 copies)
  - DHS Form 11000-6 "Conditional Access To Sensitive But Unclassified Information Non-Disclosure Agreement"
  - DHS Form 11000-9, "Disclosure and Authorization Pertaining to Consumer Report Pursuant to the Fair Credit Reporting Act"

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

- DHS may, as it deems appropriate, authorize and grant a favorable entry on duty (EOD) decision based on preliminary suitability checks. The favorable EOD decision would allow the employees 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 employment suitability authorization will follow. A favorable EOD decision or a full employment suitability 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 decision or suitability determination by the Security Office. No employee of the Contractor shall be allowed to EOD and/or access sensitive information or systems without a favorable EOD decision or suitability determination.

- Limited access to Government buildings is allowable prior to the EOD decision if the Contractor is escorted by a Government employee. This limited access is to allow Contractors to attend briefings and non-recurring meetings in order to begin transition work.

- The DHS Security Office shall be notified of all terminations /resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Technical 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 who it was issued and the last known location and disposition of the pass or card.

- When sensitive Government information is processed on Department telecommunications and automated information systems, the Contractor shall provide for the administrative control of sensitive data being processed. Contractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level. Contractors who fail to comply with Depa1iment 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).
- Failure to follow these instructions may delay the completion of suitability determinations and background checks. Note that any delays in this process that are not caused by the government do not relieve a contractor from performing under the terms of the contract.
- Your POC at the Security Office is:

  DHS OCSO/PSD Security Customer Service Center Telephone: [redacted]
  E-mailbox: [redacted]

## 11. REQUIRED REPORTS

The Contractor will notify OIDO, via the COR, of all terminations/resignations of contractor employees under the contract within five days of occurrence. The Contractor will return any expired OIDO-issued identification cards and building passes of terminated/ resigned employees to the COR. If an identification card or building pass is not available to be returned, a report must be submitted to the COR referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COR will return the identification cards and building passes to the responsible ID Unit.

The Contractor will report any adverse information coming to their attention concerning contractor employees under the contract to the OIDO, via the COR, as soon as possible. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the contractor employees' name and social security number, along with the adverse information being reported.

The Contractor will provide, through the COR a Quarterly Report containing the names of contractor employees who are active, pending hire, have departed within the quarter, or have had a legal name change (Submitted with documentation). The list shall include the Name, Position and SSN (Last Four) and should be derived from system(s) used for contractor payroll/voucher processing to ensure accuracy.

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

Sensitive information as defined under the Computer Security Act of 1987, Public Law 100-235 is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access in accordance with DHS Management Directive 11042.1, *DHS Policy for Sensitive Information.*

**12. SECURITY MANAGEMENT**

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

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

**13. INFORMATION TECHNOLOGY SECURITY CLEARANCE**

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS 4300A, Information Technology System Security Program, Sensitive Systems. Contractor employees must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

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

## 14. INFORMATION TECHNOLOGY SECURITY TRAINING AND OVERSIGHT

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

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

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

**PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL**

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

**DHS CLASS DEVIATION 15-01**
**INFORMATION TECHNOLOGY SECURITY AND PRIVACY TRAINING (MAR 2015)**

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

(b) *Security Training Requirements.*

(1) All users of Federal information systems are required by Title 5, Code of Federal Regulations, Part 930.301, Subpart C, as amended, to be exposed to security awareness materials annually or whenever system security changes occur, or when the user's responsibilities change. The Department of Homeland Security (DHS) requires that Contractor employees take an annual Information Technology Security Awareness Training course before accessing sensitive information under the contract. Unless otherwise specified, the training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall complete the training before accessing sensitive information under the contract. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. The Contractor shall

maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Unless otherwise specified, initial training certificates for each Contractor and subcontractor employee shall be provided to the Contracting Officer's Representative (COR) not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

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

(c) *Privacy Training Requirements.* All Contractor and subcontractor employees that will have access to Personally Identifiable Information (PII) and/or Sensitive PII (SPII) are required to take *Privacy at DHS: Protecting Personal Information* before accessing PII and/or SPII. The training is accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors. Training shall be completed within thirty (30) days of contract award and be completed on an annual basis thereafter not later than October 31st of each year. Any new Contractor employees assigned to the contract shall also complete the training before accessing PII and/or SPII. The Contractor shall maintain copies of training certificates for all Contractor and subcontractor employees as a record of compliance. Initial training certificates for each Contractor and subcontractor employee shall be provided to the COR not later than thirty (30) days after contract award. Subsequent training certificates to satisfy the annual training requirement shall be submitted to the COR via e-mail notification not later than October 31st of each year. The e-mail notification shall state the required training has been completed for all Contractor and subcontractor employees.

(End of clause)

**Limiting Access to Privacy Act and Other Sensitive Information**

In accordance with FAR 52.224-1 Privacy Act Notification (APR 1984), and FAR 52.224-2 Privacy Act (APR 1984), if this contract requires contractor personnel to have access to information protected by the Privacy Act of 1974, the contractor is advised that the relevant DHS system of records notices (SORNs) applicable to this Privacy Act information may be found at www.dhs.gov/privacy. Applicable SORNS of other agencies may be accessed through the

agencies' websites or by searching FDsys, the Federal Digital System, available at http://www.gpo.gov/fdsys/. SORNs may be updated at any time.

**Prohibition on Performing Work Outside a Government Facility/Network/Equipment**
The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall always remain within the confines of authorized Government networks. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall always remain within the confines of authorized Government facilities. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

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

**Separation Checklist for Contractor Employees**
Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.
In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24hours. For normal separations, the Contractor shall submit the checklist on the last day of employment or work on the contract.

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

**15. SPECIAL CLAUSES / INSTRUCTIONS**

**Compliance with DHS Security Policy Terms and Conditions:**
All hardware, software, and services provided under this task order must be compliant with *DHS 4300A, Information technology System Security Program, Sensitive Systems.*

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

## 16.0 PERIOD OF PERFORMANCE

The Task Order period of performance is for a base year plus four (4) 1-year Options.

## 17.0 PLACE OF PERFORMANCE

In-person services may be required at any location within the United States and its territories as ICE and CBP has facilities in most every state and territory.

The Contractor shall provide language services remotely via landline, cell phone, video communication (e.g., Microsoft Teams, Zoom), and mail to agency staff at any location domestically or internationally. However, linguists providing telephonic or electronic language services must be located within the continental United States and its territories (i.e., Puerto Rico, Guam, etc.).

## 18.0 TRAVEL

Travel may be required to any location within the United States and its territories. Travel may only be billed at cost in accordance with General Services Administration (GSA) Federal Travel Regulations (FTR). No Contractor profit/fee or mark-ups (such as material handling fee or general and administrative costs) may be billed to the government).

## 19.0 CONTRACT TYPE

This is a time-and-materials (T&M) contract.

## 20.0 REPORTING REQUIREMENTS

The Contractor shall provide all task order specific reports in electronic format with read/write capability using applications that are compatible with DHS workstations (i.e., Windows 7™ or later and Microsoft Office™ Applications). The task order reports listed below shall be submitted via email to the OIDO task order COR and other OIDO staff officials designated post award.

## 21.0 MONTHLY PROGRESS REPORT

The Contractor shall submit a monthly report using Microsoft Excel format and data values. The report shall include the following data elements: (1) requesting Division (2) Service Type (i.e., interpretation/translation/transcription) (3) language requested (4) total requests (5) total hours per request by language (6) total cost for each (and accumulative amount for the given performance period) (7) number of answered, abandoned, and missed calls by the Contractor (8) Connection time to linguist (9) Amount of time OIDO employees wait in que to speak with a Contractor operator. Upon award, the Contractor and OIDO will agree upon a standard format to report this information.

Separately, within the Monthly Progress Report, the average time for an OIDO employee to be connected with an interpreter upon calling the Contractor's custom number for OIDO personnel and contract staff shall be provided.

## 22.0 QUALITY CONTROL REPORT

The monthly quality control report shall include the Contractor's methodology used to monitor the quality of the work for this task order to ensure compliance with the task order' s requirements including the Performance Standards set forth in section 24.0. 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 the task order requirements.

The report shall include any changes made to the Contractors Quality Review Plan and its methodology to ensure continued compliance with the task order requirements.

## 18.0 ORGANIZATIONAL CONFLICT OF INTEREST

The Contractor shall adhere to section 15 Organizational Conflict of Interest, as outlined in the DHS Language Services BPA PWS.

## 19.0 DATA RIGHTS

Under the provisions of the Rights in Data General Clause (FAR 52.227-14), the Government reserves all rights, including copyrights, distribution rights, and other rights for all documents, data or software developed in the performance of this task order.

## 20.0 POST TASK ORDER AWARD KICK-OFF MEETING

The Contractor shall attend a post award kick-off meeting with the task order CO, COR, and other appointed representatives no later than five (5) business days after the date of award. The purpose

of this meeting is to discuss the task order, and it will be held virtually via Microsoft Teams. The Contractor shall provide a designated POC list to the COR. The COR will send a meeting invite to the Contractor for the purpose of scheduling the kick-off meeting.

## 21.0 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.

## 22.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment, and services necessary to fulfill the requirements of this task order.

## 23.0 DELIVERABLES

The Contractor shall submit electronic copies of task order deliverables listed in Table 1 to the OIDO COR for this task order in the format specified. All document deliverables for the taskorder shall be made by close of business (COB) 5:00 pm ET Monday through Friday, unless stated otherwise. All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus. All deliverables at the task order level shall be delivered in accordance with the rights set forth in FAR 52.227-17.

### Table 1: Task Order Deliverable Schedule

| Deliverable | FREQUENCY OF DELIVERY | ACCEPTABLE FORMATS | REFERENCED SECTION OF SOW |
|---|---|---|---|
| Quality Control Plan | Within 15 business days of TO award | Word/PDF | 8.0 |
| Designated POCs list | Within 3 business days after of TO award | Word/PDF | 20.0 |
| Quality Control Report | Monthly<br>Due: 10th day of each month | Word/PDF | 2.5, 17.0 |
| Monthly Progress Report | Monthly<br>Due: 15th day of each month | Excel | 16.0 |

## 24.0 PERFORMANCE STANDARDS

The Contractor shall meet the standards of performance required by OIDO. The Contractor shall be responsible for meeting the performance standards regardless of the levels of personnel qualification requirements. The performance standards that apply to this task order the Contractor shall achieve are outlined in Table 2: Task Order Performance Standards.

**Table 2: Task Order Performance Standards**

| Performance Standard | Definition | Type of Services | Minimum Acceptable Level | Method ofMonitoring |
|---|---|---|---|---|
| Confidentiality Compliance | Percentage of compliance to DHS's confidential requirements by contractor and | All | 100% | Non-disclosure agreements [ DHS Form 11000-6 (08-04)] signed by linguist |
| Certification Compliance | Percentage of compliance to DHS's certification requirements by contractor and | All | 100% | 100% inspection of documents |
| Certification of the Quality of Translated Documents | Percentage of documents being certified as accurate and reliable per DHS's requirements | All (if required) | 100% | 100% inspection of documents |
| Compliant with applicable Professional Code of Conduct and Ethics (impartiality, etc.) | Percentage of customers receives service from personnel who followapplicable professional code of conduct | All | 100% | Feedback from customers |
| Number of Complaints | Numbers of complaints receivedby the COR | All | No more than 5 complaints (overall) per month | Feedback from customers |
| Timely Delivery including timely delivery of rush requests | Percentage of deliverables that are delivered on time | All | 98% | Feedback from customers, monthly reports, submission dates |
| Responsiveness to OIDO Request(s) | Percentage of timely (w/in 3 hours) responses made by Contractor in answering OIDO's email requests | All | 95% | Feedback from customers, monthly reports, periodic surveillance, submission dates |

| | | | | |
|---|---|---|---|---|
| Overall Customer Satisfaction | Percentage of Contractor performance meeting or surpassing OIDO's contract metrics | All | 95% | Feedback from customers, Review and inspection of works and deliverables |

| | | | | |
|---|---|---|---|---|
| Speed of Connects & Call Answers | Amount of time that calls to Contractor are connected and answered by live operators | Telephonic | Callers shall reach Contractor staff (not IVR system) within 1 minute or less of connecting to the Contractor and being placed in queue. | 1. Random sampling;<br>2. Test calls;<br>3. Monthly reports;<br>Validated customer or agency complaints;<br>5. Periodic monitoring;<br>6. Submission dates;<br>7. Monthly status reviews |
| Reporting (On Time and Accuracy) | Percentage of regular or ad- hoc reports that are submitted on time | All | 95% | Feedback from COR or other designated contract representatives |
| Provision of Remedies | Percentage of corrections that are made less than 8 hours and accurately after being notified | All | 98% | Feedback from customers, submission dates, review and inspection of works and deliverables |
| Abandonment Rate | Percentage of calls that are not answered or abandoned without reaching a successful conclusion | Telephonic | Not to exceed 5% of monthly total call volume | 1. Random sampling;<br>2. Test calls;<br>3. Monthly reports;<br>4. Validated customer or agency complaints;<br>5. Periodic monitoring;<br>6. Submission dates |
| Accommodation Rate | Percentage of orders that are filled on time with a qualified linguist | All | 95% | Feedback from OIDO employees andthe Monthly |
| Contractor shall submit security packets for each of its/their interpreters that are complete to ensure compliance with security requirements. | Contractor shall submit accurate and complete security packets such that no more than five (5) security packages are incomplete each month | All | 100% | Review of incident reports (100%). |

**Table 3: Telephonic Interpreter Task Order Performance Standards**

| SSPA-1- Reporting to the Government | | | | |
|---|---|---|---|---|
| **Selected Service Performance Areas** | **Standard** | **Performance Requirement** | **Method of Surveillance** | **Performance Calculation** |
| **1.1** For all calls, gather the required information from callers, including OIDO personnel name, OIDO Division, location, Contractor Interpreter ID, and language for each call. | Required information shall be collected for each call. | Less than 2% of total monthly calls shall have this data omitted. | 1. Random sampling<br>2. Test calls<br>3. Monthly reports<br>4. Periodic monitoring<br>5. Management reports<br>6. Status reviews<br><br>Period: Monthly | Will be noted in CPARS review |

| SSPA-2 - Maintain constant availability to Systems | | | | |
|---|---|---|---|---|
| **Selected Service Performance Areas** | **Standard** | **Performance Requirement** | **Method of Surveillance** | **Performance Calculation** |
| 2.1 Maintain constant availability to systems.<br><br>[Defined: Systems are defined as all telephone, IT and other platforms or connectivity necessary for OIDO staff to reach an interpreter as well as real-time reporting tool for designated officials]. | Systems are available to OIDO 24 hours a day, 7 days a week, and 365 days a year (24/7/365). | Systems shall be available to OIDO at all times. | 1. Random sampling<br>2. Test calls<br>3. Contractor reports<br><br>Period: Monthly | |

| SSPA-3 – Customer Service | | | | |
|---|---|---|---|---|
| **Selected Service Performance Areas** | **Standard** | **Performance Requirement** | **Method of Surveillance** | **Performance Calculation** |

| | | | | |
|---|---|---|---|---|
| **3.1** Customer Service | Customers receive professional and polite service from Contractor.<br><br>Contractors shall only interpret word for word. | No more than 5 complaints may be received during the month. | 11. Random sampling<br>12. Test calls<br>13. Monthly reports<br>14. Validated customer or agency complaints<br><br>Period: Monthly | Corrective Action Plan must be provided to COR if more than 5 complaints regarding the same topic are received in a given month. |
| **SSPA-4 –Speed of Connects** | | | | |
| **Selected Service Performance Areas** | **Standard** | **Performance Requirement** | **Method of Surveillance** | **Performance Calculation** |
| **4.1-** Speed of connects<br><br>Defined: Speed of connect time is calculated from when the language is requested by OIDO until the call reaches the interpreter. | Calls shall be answered by an interpreter in the specified monthly aggregate time frames for the following languages:<br><br>**Tier 1 languages see Appendix B: Haitian/Creole, Mandarin, Portuguese, Punjabi, Spanish**<br>Average connect time within 60 seconds | **Tier 1 languages**<br><br>Monthly average connect time for Haitian/Creole, Mandarin, Portuguese, Punjabi, and Spanish calls must be 60 seconds or less. | 1. Random sampling<br>2. Test calls<br>3. Monthly Progress Report<br>4. Validated customer or agency complaints<br><br>Period: Monthly | **Tier 1 languages**<br><br>Deduct 10% from the total monthly cost of Tier 1 calls if monthly average connect time is greater than 60 seconds but less than 70 seconds.<br><br>Deduct 20% from the total monthly cost of Tier 1 calls if monthly average connect time is 70 seconds or greater. |

| | | | | |
|---|---|---|---|---|
| | **Tier 2 languages see Appendix B**<br><br>Average connect time within 3 minutes for languages "requested most often".<br><br>**Tier 3 languages see Appendix B**<br><br>Average connect time within 5 minutes for italicized languages "languages requested least often".<br><br>For italicized languages "requested least often", an 8-hour response time is acceptable. Email notification must be given to the requestor when a linguist will be available. | **Tier 2 languages**<br><br>Monthly average connect time for all Tier 2 calls must be 3 minutes or less.<br><br>**Tier 3 languages**<br><br>Monthly average connect time for italicized languages must be 5 minutes or less. | | **Tier 2 languages**<br><br>Deduct 10% from the total monthly cost of Tier 2 calls if monthly average connect time is greater than 3 minutes but less than 4 minutes.<br><br>Deduct 20% from the total monthly cost of Tier 2 calls if monthly average connect time is 4 minutes or greater.<br><br>**Tier 3 languages**<br><br>Will be noted in CPARS review if standard is not met. No more than 5% of calls should exceed the requested time frame. |
| **SSPA 5 – Translation Turnaround** | | | | |
| **Selected Service Performance Areas** | **Standard** | **Performance Requirement** | **Method of Surveillance** | **Performance Calculation** |

| | | | | |
|---|---|---|---|---|
| **5.1-** Translation Turnaround<br><br>[Defined: Translation turnaround time is calculated from when the translation request is received by the Contractor (coordinator, designated mailbox, etc.) until the translated written document or audio recording (see 3.2 Foreign Language Translation for full listing of documents/recordings) is received by OIDO. | Translations shall be received by an interpreter in the specified monthly aggregate time frames for the following languages:<br><br>**Tier 1 languages**<br>**Haitian/Creole, Mandarin, Portuguese, Punjabi, Spanish** (see Appendix A )<br>Average translation turnaround time is within 3 business days.<br><br>**Tier 2 languages**<br>Average translation turnaround time for languages "requested most often" is within 5 business days.<br><br>**Tier 3 languages**<br>Average translation turnaround time is within 7 business days for italicized "languages requested least often".<br><br>For certain indigenous languagesthere is no written form hence no translation will be required. | **Tier 1 languages**<br><br>Monthly average translation turnaround time is within 3 business days.<br><br>**Tier 2 languages**<br><br>Monthly average translation turnaround time is within 5 business days.<br><br>**Tier 3 languages**<br>Monthly average translation turnaround time is within 7 business days. | 1. Random sampling<br>2. Test calls<br>3. Monthly Progress Report<br>4. Validated customer or agency complaints<br><br>Period: Monthly | **Tier 1 languages**<br><br>Deduct 10% from the total monthly cost of Tier 1 languages if monthly average translation turnaround time is greater than 3 business days but less than 5 business days.<br><br>**Tier 2 languages**<br><br>Will be noted in CPARS review if standard is not met. No more than 5% of translation requests should exceed the requested time frame.<br><br>**Tier 3 languages**<br>Will be noted in CPARS review if standard is not met. No more than 5% of translation requests should exceed the requested time frame. |
| **SSPA 6 – Contractor personnel are properly adjudicated** | | | | |

| Selected Service Performance Areas | Standard | Performance Requirement | Method of Surveillance | Performance Calculation |
|---|---|---|---|---|
| **6.1** All personnel interpreting data shall be successfully adjudicated and e-QIP cleared for Public Trust Positions at an MBI level. | All calls shall be interpreted by personnel cleared by DHS for public trust positions (MBI). | No calls shall be answered by an interpreter without being vetted (fingerprinted/e-QIP). | Random sampling of call activity Monthly/ Daily reports. | This is grounds for Termination for Cause. |

| SSPA 7 – Access with minimal in queue times | | | | |
|---|---|---|---|---|
| **Selected Service Performance Areas** | **Standard** | **Performance Requirement** | **Method of Surveillance** | **Performance Calculation** |
| **7.1** Callers shall have access to language interpreters 24 /7 /365 with minimal time in queue.<br><br>[Defined: Queue is the time prior to language identification by the Contractor] | Callers shall be in queue less than 60 seconds. | Callers shall reach Contractor personnel (not IVR system) within 1 minute or less of connecting to the Contractor's phone system and being placed in queue. | 1. Test calls<br>2. Validated customer or agency complaints<br>3. Periodic monitoring<br>4. Monthly Progress Reports | If more than 5% of monthly calls exceed a 1-minute que time, a corrective action plan must be created to resolve the issue. |
| **SSPA 8 –All OIDO calls shall reach language interpreter on a continuous basis.** | | | | |
| **Selected Service Performance Areas** | **Standard** | **Performance Requirement** | **Method of Surveillance** | **Performance Calculation** |
| **8.1 All** OIDO callers shall reach a language interpreter on a continuous 24/7/365 basis and within the connect time specified in the language Tier requirements regardless of time of day, weekend or holiday. | All callers shall reach a linguist. Defined: Calls that do not reach an interpreter **include but are not limited to:** calls that are deflected receive busy signals or high call volume messages, are placed on hold for longer than the language Tier connect time, and calls during which the caller hangs up or does not reach an interpreter. | Calls that do not reach an interpreter shall be less than 3% of monthly total call volume. | 1. Test calls<br>2. Validated customer or agency complaint<br>3. Periodic surveillance<br>4. Monthly Progress Reports | If more than 5% of calls do not reach an interpreter due to a Contractor issue, a corrective action plan must be created. |

## PRIVACY REQUIREMENTS FOR CONTRACTOR AND PERSONNEL

In addition to FAR 52.224-1 Privacy Act Notification (APR 1984), 52.224-2 Privacy Act (APR 1984), FAR 52.224-3 Privacy Training (JAN 2017), and HSAR Clauses, the following instructions must be included in their entirety in all contracts.

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

**Prohibition on Performing Work Outside a Government Facility/Network/Equipment**
The Contractor shall perform all tasks on authorized Government networks, using Government-furnished IT and other equipment and/or Workplace as a Service (WaaS) if WaaS is authorized by the statement of work. Government information shall remain within the confines of authorized Government networks at all times. Except where telework is specifically authorized within this contract, the Contractor shall perform all tasks described in this document at authorized Government facilities; the Contractor is prohibited from performing these tasks at or removing Government-furnished information to any other facility; and Government information shall remain within the confines of authorized Government facilities at all times. Contractors may only access classified materials on government furnished equipment in authorized government owned facilities regardless of telework authorizations.

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

**Separation Checklist for Contractor Employees**
Contractor shall complete a separation checklist before any employee or Subcontractor employee terminates working on the contract. The separation checklist must verify: (1) return of any Government-furnished equipment; (2) return or proper disposal of sensitive personally identifiable information (PII), in paper or electronic form, in the custody of the employee or Subcontractor employee including the sanitization of data on any computer systems or media as appropriate; and (3) termination of any technological access to the Contractor's facilities or systems that would permit the terminated employee's access to sensitive PII.
In the event of adverse job actions resulting in the dismissal of an employee or Subcontractor employee, the Contractor shall notify the Contracting Officer's Representative (COR) within 24 hours. For normal separations, the Contractor shall submit the checklist on the last day of

employment or work on the contract.

**Contractor's Commercial License Agreement and Government Electronic Information Rights**

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

**Privacy Lead Requirements**

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

The Privacy Lead:

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

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

that questions asked by the DHS PSO and other offices are answered in a timely fashion.

## SAFEGUARDING OF SENSITIVE INFORMATION (MAR 2015)

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

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

"Personally Identifiable Information (PII)" means information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-personally identifiable information can become personally identifiable information whenever additional information is made publicly available—in any medium and from any source—that, combined with other available information, could be used to identify an individual.

PII is a subset of sensitive information. Examples of PII include, but are not limited to: name, date of birth, mailing address, telephone number, Social Security number (SSN), email address, zip code, account numbers, certificate/license numbers, vehicle identifiers including license plates, uniform resource locators (URLs), static Internet protocol addresses, biometric identifiers such as fingerprint, voiceprint, iris scan, photographic facial images, or any other unique identifying number or characteristic, and any information where it is reasonably foreseeable that the information will be linked with other information to identify the individual.

"Sensitive Information" is defined in HSAR clause 3052.204-71, Contractor Employee Access, as any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, Part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," 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 his/her designee);

(3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

(4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.

"Sensitive Information Incident" is an incident that includes the known, potential, or suspected exposure, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or unauthorized access or attempted access of any Government system, Contractor system, or sensitive information.

"Sensitive Personally Identifiable Information (SPII)" is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements. Examples of such PII include: Social Security numbers (SSN), driver's license or state identification number, Alien Registration Numbers (A-number), financial account number, and biometric identifiers such as fingerprint, voiceprint, or iris scan. Additional examples include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

(1) Truncated SSN (such as last 4 digits)
(2) Date of birth (month, day, and year)
(3) Citizenship or immigration status
(4) Ethnic or religious affiliation
(5) Sexual orientation
(6) Criminal History
(7) Medical Information
(8) System authentication information such as mother's maiden name, account passwords or personal identification numbers (PIN)

Other PII may be "sensitive" depending on its context, such as a list of employees and their performance ratings or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII but is not sensitive.

(c) *Authorities.* The Contractor shall follow all current versions of Government policies and guidance accessible at http://www.dhs.gov/dhs-security-and-training-requirements-contractors, or available upon request from the Contracting Officer, including but not limited to:

(1) DHS Management Directive 11042.1 Safeguarding Sensitive But Unclassified (for Official Use Only) Information
(2) DHS 4300A, Information Technology System Security Program, Sensitive Systems
(3) DHS Security Authorization Process Guide
(4) DHS Instruction 121-01-007-01, Revision 01, The Department of Homeland Security Personnel Security, Suitability and Fitness Program
(5) DHS Information Security Performance Plan (current fiscal year)
(6) DHS Privacy Incident Handling Guidance
(7) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(8) National Institute of Standards and Technology (NIST) Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations accessible at http://csrc.nist.gov/publications/PubsSPs.html
(9) NIST Special Publication 800-88 Guidelines for Media Sanitization accessible at http://csrc.nist.gov/publications/PubsSPs.html

(d) *Handling of Sensitive Information.* Contractor compliance with this clause, as well as the policies and procedures described below, is required.

(1) Department of Homeland Security (DHS) policies and procedures on Contractor personnel security requirements are set forth in various Management Directives (MDs), Directives, and Instructions. *MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use Only) Information* describes how Contractors must handle sensitive but unclassified information. DHS uses the term "FOR OFFICIAL USE ONLY" to identify sensitive but unclassified information that is not otherwise categorized by statute or regulation. Examples of sensitive information that are categorized by statute or regulation are PCII, SSI, etc. The *DHS Sensitive Systems Policy Directive 4300A.* The *DHS 4300A, Information Technology System Security Program, Sensitive Systems. DHS Instruction 121-01-007-01, Revision 01, The Department of Homeland Security Personnel Security, Suitability and Fitness Program* establishes that DHS Components ensure that only United States (U.S.) Citizens are granted access to DHS systems and networks.

(2) The Contractor shall not use or redistribute any sensitive information processed, stored, and/or transmitted by the Contractor except as specified in the contract.

(3) All Contractor employees with access to sensitive information shall execute *DHS Form 11000-6, Department of Homeland Security Non-Disclosure Agreement (NDA),* as a condition of access to such information. The Contractor shall maintain signed copies of the NDA for all employees as a record of compliance. The Contractor shall provide copies of the signed NDA to the Contracting Officer's Representative (COR) no later than two (2) days after execution of the form.

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

(e) *Authority to Operate*. The Contractor shall not input, store, process, output, and/or transmit sensitive information within a Contractor IT system without an Authority to Operate (ATO) signed by the Headquarters or Component CIO, or designee, in consultation with the Headquarters or Component Privacy Officer. Unless otherwise specified in the ATO letter, the ATO is valid for three (3) years. The Contractor shall adhere to current Government policies, procedures, and guidance for the Security Authorization (SA) process as defined below.

(1) Complete the Security Authorization process. The SA process shall proceed according to the *DHS 4300A, Information Technology System Security Program, Sensitive Systems,* (Version 13.3, February 13, 2023).

(i) Security Authorization Process Documentation. SA documentation shall be developed using the Government provided Requirements Traceability Matrix and Government security documentation templates. SA documentation consists of the following: Security Plan, Contingency Plan, Contingency Plan Test Results, Configuration Management Plan, Security Assessment Plan, Security Assessment Report, and Authorization to Operate Letter. Additional documents that may be required include a Plan(s) of Action and Milestones and Interconnection Security Agreement(s). During the development of SA documentation, the Contractor shall submit a signed SA package, validated by an independent third party, to the COR for acceptance by the Headquarters or Component CIO, or designee, at least thirty (30) days prior to the date of operation of the IT system. The Government is the final authority on the compliance of the SA package and may limit the number of resubmissions of a modified SA package. Once the ATO has been accepted by the Headquarters or Component CIO, or designee, the Contracting Officer shall incorporate the ATO into the contract as a compliance document. The Government's acceptance of the ATO does not alleviate the Contractor's responsibility to ensure the IT system controls are implemented and operating effectively.

(ii) Independent Assessment. Contractors shall have an independent third party validate the security and privacy controls in place for the system(s). The independent third party shall review and analyze the SA package, and report on technical, operational, and management level deficiencies as outlined in *NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations*. The Contractor shall address all deficiencies before submitting the SA package to the Government for acceptance.

(iii) Support the completion of the Privacy Threshold Analysis (PTA) as needed. As part of the SA process, the Contractor may be required to support the Government in the completion of the PTA. The requirement to complete a PTA is triggered by the creation, use, modification, upgrade, or disposition of a Contractor IT system that will store, maintain and use PII, and must be renewed at least every three (3) years. Upon review of the PTA, the

DHS Privacy Office determines whether a Privacy Impact Assessment (PIA) and/or Privacy Act System of Records Notice (SORN), or modifications thereto, are required. The Contractor shall provide all support necessary to assist the Department in completing the PIA in a timely manner and shall ensure that project management plans and schedules include time for the completion of the PTA, PIA, and SORN (to the extent required) as milestones. Support in this context includes responding timely to requests for information from the Government about the use, access, storage, and maintenance of PII on the Contractor's system, and providing timely review of relevant compliance documents for factual accuracy. Information on the DHS privacy compliance process, including PTAs, PIAs, and SORNs, is accessible at http://www.dhs.gov/privacy-compliance.

(2) *Renewal of ATO.* Unless otherwise specified in the ATO letter, the ATO shall be renewed every three (3) years. The Contractor is required to update its SA package as part of the ATO renewal process. The Contractor shall update its SA package by one of the following methods: (1) Updating the SA documentation in the DHS automated information assurance tool for acceptance by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls; or (2) Submitting an updated SA package directly to the COR for approval by the Headquarters or Component CIO, or designee, at least 90 days before the ATO expiration date for review and verification of security controls. The 90 day review process is independent of the system production date and therefore it is important that the Contractor build the review into project schedules. The reviews may include onsite visits that involve physical or logical inspection of the Contractor environment to ensure controls are in place.

(3) *Security Review.* The Government may elect to conduct random periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, the Office of the Inspector General, and other Government organizations access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor shall, through the Contracting Officer and COR, contact the Headquarters or Component CIO, or designee, to coordinate and participate in review and inspection activity by Government organizations external to the DHS. Access shall be provided, to the extent necessary as determined by the Government, for the Government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of Government data or the function of computer systems used in performance of this contract and to preserve evidence of computer crime.

(4) *Continuous Monitoring.* All Contractor-operated systems that input, store, process, output, and/or transmit sensitive information shall meet or exceed the continuous monitoring requirements identified in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The plan is updated on an annual basis. The Contractor shall also store monthly continuous monitoring data at its location for a period not less than one year from the date the data is created. The data shall be encrypted in accordance with *FIPS 140-2 Security Requirements for Cryptographic Modules* and shall not be stored on systems that are shared with other commercial or Government entities. The Government may elect to perform continuous monitoring and IT security scanning of Contractor systems from Government tools and

infrastructure.

(5) *Revocation of ATO.* In the event of a sensitive information incident, the Government may suspend or revoke an existing ATO (either in part or in whole). If an ATO is suspended or revoked in accordance with this provision, the Contracting Officer may direct the Contractor to take additional security measures to secure sensitive information. These measures may include restricting access to sensitive information on the Contractor IT system under this contract. Restricting access may include disconnecting the system processing, storing, or transmitting the sensitive information from the Internet or other networks or applying additional security controls.

(6) *Federal Reporting Requirements.* Contractors operating information systems on behalf of the Government or operating systems containing sensitive information shall comply with Federal reporting requirements. Annual and quarterly data collection will be coordinated by the Government. Contractors shall provide the COR with requested information within three (3) business days of receipt of the request. Reporting requirements are determined by the Government and are defined in the *Fiscal Year 2014 DHS Information Security Performance Plan,* or successor publication. The Contractor shall provide the Government with all information to fully satisfy Federal reporting requirements for Contractor systems.

(f) *Sensitive Information Incident Reporting Requirements.*

(1) All known or suspected sensitive information incidents shall be reported to the Headquarters or Component Security Operations Center (SOC) within one hour of discovery in accordance with *4300A Sensitive Systems.* When notifying the Headquarters or Component SOC, the Contractor shall also notify the Contracting Officer, COR, Headquarters or Component Privacy Officer, and US-CERT using the contact information identified in the contract. If the incident is reported by phone or the Contracting Officer's email address is not immediately available, the Contractor shall contact the ContractingOfficer immediately after reporting the incident to the Headquarters or Component SOC. The Contractor shall not include any sensitive information in the subject or body of any e-mail. To transmit sensitive information, the Contractor shall use *FIPS 140-2 Security Requirements for Cryptographic Modules* compliant encryption methods to protect sensitive information in attachments to email. Passwords shall not be communicated in the same email as the attachment.A sensitive information incident shall not, by itself, be interpreted as evidence that the Contractorhas failed to provide adequate information security safeguards for sensitive information, or has otherwise failed to meet the requirements of the contract.

(2) If a sensitive information incident involves PII or SPII, in addition to the reporting requirements in *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) Data Universal Numbering System (DUNS);
(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, email);
(v) Contracting Officer POC (address, telephone, 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 sensitive information resided at the time of the incident, both at the Contractor and subcontractor level;
(xii) Description of the Government PII and/or SPII contained within the system;
(xiii) Number of people potentially affected and the estimate or actual number of records exposed and/or contained within the system; and
(xiv) Any additional information relevant to the incident.

(g) *Sensitive Information Incident Response Requirements.*

(1) All determinations related to sensitive information incidents, including response activities, notifications to affected individuals and/or Federal agencies, and related services (e.g., credit monitoring) will be made in writing by the Contracting Officer in consultation with the Headquarters or Component CIO and Headquarters or Component Privacy 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 sensitive information 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, and
(iv) Data analyses and processing.

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

(h) *Additional PII and/or SPII Notification Requirements*.

(1) The Contractor shall have in place procedures and the capability to notify any individual whose PII resided in the Contractor IT system at the time of the sensitive information incident not later than 5 business days after being directed to notify individuals, unless otherwise

approved by the Contracting Officer. The method and content of any notification by the Contractor shall be coordinated with, and subject to prior written approval by the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, utilizing the *DHS Privacy Incident Handling Guidance*. The Contractor shall not proceed with notification unless the Contracting Officer, in consultation with the Headquarters or Component Privacy Officer, has determined in writing that notification is appropriate.

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

(i) A brief description of the incident;
(ii) A description of the types of PII and SPII involved;
(iii) A statement as to whether the PII or SPII was encrypted or protected by other means;
(iv) Steps individuals may take to protect themselves;
(v) What the Contractor and/or the Government are doing to investigate the incident, to mitigate the incident, and to protect against any future incidents; and
(vi) Information identifying who individuals may contact for additional information.

(i) *Credit Monitoring Requirements*. In the event that a sensitive information incident involves PII or SPII, the Contractor may be required to, as directed by the Contracting Officer:

(1) Provide notification to affected individuals as described above; and/or

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

(i) Triple credit bureau monitoring;
(ii) Daily customer service;
(iii) Alerts provided to the individual for changes and fraud; and
(iv) Assistance to the individual with enrollment in the services and the use of fraud alerts; and/or

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

(i) A dedicated telephone number to contact customer service within a fixed period;
(ii) Information necessary for registrants/enrollees to access credit reports and credit scores;

(iii) Weekly reports on call center volume, issue escalation (i.e., those calls that cannot be handled by call center staff and must be resolved by call center management or DHS, as appropriate), and other key metrics;
(iv) Escalation of calls that cannot be handled by call center staff to call center management or DHS, as appropriate;
(v) Customized FAQs, approved in writing by the Contracting Officer in coordination with the Headquarters or Component Chief Privacy Officer; and
(vi) Information for registrants to contact customer service representatives and fraud resolution representatives for credit monitoring assistance.

(j) *Certification of Sanitization of Government and Government-Activity-Related Files and Information.* As part of contract closeout, the Contractor shall submit the certification to the COR and the Contracting Officer following the template provided in *NIST Special Publication 800-88 Guidelines for Media Sanitization*.

(End of clause)

**A.1 In accordance with ITAR 4.5.3.1 – Compliance with DHS Security Policy Terms and Conditions.**

**Compliance with DHS Security Policy Terms and Conditions:**

All hardware, software, and services provided under this task order must be compliant with *DHS 4300A, Information Technology System Security Program, Sensitive Systems policy.*

**A.2 In accordance with ITAR 4.5.3.4 and ITAR 4.5.4.4 – Security Review**

**Security Review Terms and Conditions**

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

## Appendix A
## List of Languages Previously Encountered – Translation & Transcription

| Language | Language | Language |
|---|---|---|
| Afrikaans | Czech | Hmong |
| **Albanian (incl. Cham dialect)** | Danish | **Hungarian** |
| Amharic | *Dari* | *Ibo* |
| **Arabic** | Daril/Tajiki | Icelandic |
| Armenian | *Dhivehi / Maldivian* | Igbo |
| *Assamese* | *Dhundhari* | Ilocano |
| Assyrian | Dinka | Indonesian |
| Azeri/Azerbaijani | *Divehi* | Iraqi |
| Bahasa | Dominican Republic Native | Irish |
| Baloch | *Doula* | **Italian** |
| Balochi | *Duala* | **Japanese** |
| Baluchi | Dutch | Javanese |
| Basque | *EBONIC* | Kachin |
| *Bassa* | English | Kackchiquel |
| Belorussian | Estonian | Kanjobal |
| **Bengali** | Ewe | Kannada |
| Berber dialects | *Ewondo* | Kashmiri |
| Bosnian | **Farsi** | Kazakh |
| Bosnian-Croatian | Fijian | Khirghiz |
| Braille | Filipino/Tagalog/Pilipino/Philippine | Khmer |
| Bulgarian | Finnish | Kiknogo/Kingiona |
| Burmese | Flemish | Kinyarwanda |
| Byelorussian | *Fon* | *Kirindi* |
| Cambodian | **French** | Krio |
| **Cantonese** | French Patois | Kurdish |
| Catalan | French, Canadian | *Kurdish Sorani* |
| Cebuano/Visayan | Fu lani/Hasua/Ibo/Yoruba | Kurmanci |
| Chadic | Ga | Kyrgyz |
| Chaldeen | *Gaelic* | Lao |
| Chamorro | Georgian | **Lao/Laotian** |
| Chao-Chow | **German** | Lapp |
| *Chechen* | *Grebo* | *Latin* |
| *Cherokee* | Greek | Latvian |
| Chichewa | *Guarani* | Lebanese |
| Chimora | Gujarati | *Liberian* |
| **Chinese (Simplified)** | Guyanese | Lingala |
| **Chinese (Traditional)** | Haitian Creole/Haitian/Kreyol | Lithuanian |
| **Creole** | Hausa | Luxembourgisch |
| Creole Patois | Hebrew | Macedonian |
| Croatian | **Hindi** | Malagasy |

Legend

| **Language Requested Most Often** | *Language Requested Least Often* |
|---|---|

****Appendix A is not inclusive of all languages that DHS may need to acquire for operation.**

## Appendix A
## List of Languages Previously Encountered – Translation & Transcription (Cont'd)

| Language | Language | Language |
|---|---|---|
| Malay | Quiche | Tibetan |
| Malayalam | Romani | *Tigre* |
| Malaya-Polynesian | *Romani* | Tigrinya |
| Malaysian | Romanian | Tigrinya/Eritrean |
| Maltese | **Russian** | Toishanese |
| Mam | Samoan | Tongan |
| Mandalay | *Sango* | Toucouleur |
| *Mandingo* | Sanskrit | *Tsongo* |
| Marathi | Serbian | Turkic |
| *Masai* | Serbo | Turkish |
| *Mayan* | Serbo Croatian | Turkmen |
| Minbei (Fuzhou) | Shan | Turkmen/Turkmenian |
| Minnan (Hokkien-Taiwanese) | Shona | Twi |
| *Miskito* | Sindhalese | Twi/Akan/Fante |
| Moldovan | Sindhi | Ukrainian |
| Mon | Sinhala | **Urdu** |
| Mongolian/Khalkha Mongolian | Sinhala/Sinhalese | *Uyghur* |
| Mon-Khmer | Slovak | Uzbek |
| Moshi-Dagomba | Slovenian/Slovene | **Vietnamese (incl. Cochinchinese)** |
| *Navajo* | Somali | Welsh |
| *Ndebele* | *Soninke/Sarahule* | Wolof |
| **Nepali/Nepalese** | Sotho | Xhosa |
| *Nigerian* | **South Korean** | Xiang |
| *North Korean* | **Spanish** | Yiddish |
| Norwegian | Spanish, Castilian | Yoruba |
| *Nuer* | Suriname Tongo | Yugoslavian |
| Oromo | Swahili | Yunnanese |
| *Palauan* | Swedish | Zulu |
| Papiamento | *Syriac* | |
| Pashai | Tadjik/Tadzhik | |
| Pashtu/Pashto | Tagalog | |
| Patois | Tajik | |
| Persian | Taki-Taki | |
| **Polish** | *Tamang* | |
| Portuguese | Tamil | |
| **Portuguese, Continental** | Tatar | |
| Potwa (Jamaican Patois) | Tausug | |
| **Punjabi** | Telugu | |
| Qanjobal/Kanjobal | **Thai** | |

Legend

| **Language Requested Most Often** | *Language Requested Least Often* |
|---|---|

****Appendix A is not inclusive of all languages that DHS may need to acquire for operation.**

## Appendix B
## List of Languages Previously Encountered – Interpretation

| Language | Language | Language |
|---|---|---|
| *African French* | Croatian | Hakka dialects |
| Afrikaans | Czech | Hausa |
| Albanian (incl. Cham dialect) | Danish | Hebrew |
| Amharic | *Dari* | Hindi |
| **Arabic** | Daril/Tajiki | Hmong |
| *Arabic dialects (e.g. Yemeni, Iraq, etc)* | *Dhivehi / Maldivian* | Hungarian |
| Armenian | *Dhundhari* | *Ibo* |
| *Assamese* | Dinka | Icelandic |
| Assyrian | *Divehi* | Igbo |
| Azeri/Azerbaijani | Dominican Republic Native | Ilocano |
| Bahasa | *Doula* | Indonesian |
| Baloch | *Duala* | Iraqi |
| Balochi | Dutch | Irish |
| Baluchi | *EBONIC* | Italian |
| *Bambara* | Estonian | Japanese |
| Basque | Ewe | Javanese |
| *Bassa* | *Ewondo* | Kachin |
| Belorussian | **Farsi** | Kackchiquel |
| Bengali | Fijian | Kanjobal |
| Berber dialects | Filipino/Tagalog/Pilipino/Philippine | Kannada |
| Bosnian | Finnish | Kashmiri |
| Bosnian-Croatian | Flemish | Kazakh |
| Braille | *Fon* | Khirghiz |
| Bulgarian | **French** | Khmer |
| Burmese | French Patois | Kiknogo/Kingiona |
| Byelorussian | French, Canadian | Kinyarwanda |
| Cambodian | Fu lani/Hasua/Ibo/Yoruba | *Kirindi* |
| **Cantonese/Yue** | Fukien/Fukienese | **South Korean** |
| Catalan | Fuzchou | Krio |
| Cebuano/Visayan | Fuzchou/Fuzhou/Foo Chow | Kurdish |
| Chadic | Ga | *Kurdish Sorani* |
| Chaldeen | *Gaelic* | Kurmanci / Kurdish Kurmanji |
| Chamorro | Georgian | Kyrgyz |
| Chao-Chow | German | Lao |
| *Chechen* | *Grebo* | Lao/Laotian |
| *Cherokee* | Greek | Lapp |
| Chichewa | *Guarani* | *Latin* |
| Chimora | Gujarati | Latvian |
| Chin | Guyanese | Lebanese |
| Creole | Haitian Creole/Haitian/Kreyol/Creole | *Levantine Arabic* |
| Creole Patois | Hakka | *Liberian* |

Legend

| Language Requested Most Often | *Language Requested Least Often* |
|---|---|

****Appendix B is not inclusive of all languages that DHS may need to acquire for operation.**

## Appendix B
## List of Languages Previously Encountered – Interpretation (Cont'd)

| Language | Language | Language |
|---|---|---|
| Lingala | Polish | Tajik |
| Lithuanian | **Portuguese** | Taki-Taki |
| Luxembourgisch | *Portuguese dialects* | *Tamang* |
| Macedonian | Portuguese, Continental | Tamil |
| Malagasy | Potwa (Jamaican Patois) | Tatar |
| Malay | **Punjabi** | Tausug |
| Malayalam | Qanjobal/Kanjobal | Telugu |
| Malaya-Polynesian | Quiche | Thai |
| Malaysian | Romani | Tibetan |
| Maltese | *Romani* | *Tigre* |
| Mam | Romanian | Tigrinya |
| Mandalay | **Russian** | Tigrinya/Eritrean |
| **Mandarin (Chinese)** | Samoan | Toishanese |
| *Mandingo* | *Sango* | Tongan |
| Marathi | Sanskrit | Toucouleur |
| *Masai* | Serbian | *Tsongo* |
| *Mayan* | Serbo | Turkic |
| Minbei (Fuzhou) | Serbo Croatian | Turkish |
| Minnan (Hokkien-Taiwanese) | Shan | Turkmen |
| *Miskito* | Shona | Turkmen/Turkmenian |
| Moldovan | *Sicilian* | Twi |
| Mon | Sindhalese | Twi/Akan/Fante |
| Mongolian/Khalkha Mongolian | Sindhi | Ukrainian |
| Mon-Khmer | Sinhala | Urdu |
| Moshi-Dagomba | Sinhala/Sinhalese | *Uyghur* |
| *Navajo* | Slovak | Uzbek |
| *Ndebele* | Slovenian/Slovene | **Vietnamese (incl. Cochinchinese)** |
| Nepali/Nepalese | Somali | Welsh |
| *Nigerian* | *Soninke/Sarahule* | Wenzhou |
| *North Korean* | Sotho | Wolof |
| Norwegian | **Spanish** | Wu (Shanghainese) |
| Not Specified | Spanish, Castilian | Xhosa |
| *Nuer* | *Sudanese Arabic* | Xiang |
| Oromo | Suriname Tongo | Yiddish |
| *Palauan* | Swahili | Yoruba |
| Papiamento | Swedish | Yugoslavian |
| Pashai | *Syriac* | Yunnanese |
| Pashtu/Pashto | Tadjik/Tadzhik | Zulu |
| Patois | Tagalog | |
| Persian | Taiwanese | |

Legend

| **Language Requested Most Often** | *Language Requested Least Often* |
|---|---|

****Appendix B is not inclusive of all languages that DHS may need to acquire for operation.**

## Appendix C
## Examples of Uncommon and Rare Languages and Dialects

1. Quechua
2. Bantu
3. Akatek/Acateco
4. Hassaniya
5. Kirundi
6. Jula/Dyula
7. Garifuna
8. Garafuna
9. Kiswahili
10. Malinke
11. Mina
12. Moghamo
13. Zomi
14. Achi
15. Chuj
16. Ixil
17. Popti

*Appendix C is not inclusive of all uncommon and rare languages that DHS may need to acquirefor operation