SECTION II – STATEMENT OF WORK

The Department of Homeland Security
Office for Civil Rights and Civil Liberties
Language Services

September 2022

1.0 GENERAL

1.1 Background

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

To fulfill the DHS mandates in all aspects of this homeland security enterprise, DHS requires ready access to a comprehensive set of high-quality language services for interactions with individuals whom DHS serves and encounters. This must include the full array of language services to ensure effective communication with persons who are non-or- limited English speaking (e.g., foreign language interpretation; translations) and those who have a range of communication access needs, and other language services that support DHS in carrying out specific law enforcement activities and promotes compliance with federal civil rights requirements.

2. Scope

The purpose of this contract is to obtain high quality timely services to carry out the mission of CRCL ensuring meaningful access to Limited English Proficient (LEP) persons to the programs, services and activities of the Department. In order to fulfill CRCL's mission, the office requires access to language services delivered via methods to include, but not limited to, Foreign Language Translation, Foreign Language Interpretation, including onsite, telephonic, virtual, voiceover and sight translation, Transcription Translation/Captioning Services; Desktop Publishing, including 508 compliance for all deliverables when required. Contractor services shall include, but are not limited to, providing quality language translation of any written materials and interpretation services in the full range of languages likely to be encountered in the United States.

3.0 REQUIREMENTS

3.1 The Contractor shall provide language services through qualified linguists as specified in the general requirements for the DHS Language Services II Performance Work Statement.

3.2 CRCL 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 homeland security language needs.

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. This includes rapid deployment of linguists to the place of performance set forth in a task order which may include Government, Non-Government, and Contractor sites (including teleworking sites) within 24-hour notice.

3.3 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 travel shall not be charged to CRCL.

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

3.5 The Contractor shall have the capability of telecommunication technology (i.e., landline and cell phone, email, fax (machine or electronic), basic internet which may include virtual connectivity to applications such as, but not limited to, Microsoft Teams and Zoom, to provide services.

3.6 The Contractor shall provide and maintain a secure, web-based interface/portal which allows access to call order performance data. The portal shall be available to the CRCL COR to conveniently generate reports, analysis, and other self- produced ad-hoc queries. Performance data shall be maintained in 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.

3.7 The Contractor shall provide a staffing and recruitment plan detailing how linguists will be recruited, trained, and retained locally and nationally to ensure CRCL's needs (e.g. "steady state" and "surge" requirements) are met, with a special emphasis on on-site services for remote locations. The Contractor shall also include a contingency plan for replacing or substituting linguists when the ones originally assigned to the call orders are not able to perform or meet the call order requirements.

4.0 LANGUAGE SERVICES REQUIRED

The languages most frequently encountered language by CRCL is Spanish; however, CRCL requires translation and interpreter services in many other languages (samples of which are listed in Appendix A). Therefore, the contractor must be prepared to serve LEP persons in any languages that may be encountered in the United States.

4.1 Foreign Language Translation

CRCL requires translation of many kinds of written documents, including but not limited to forms, instructions, websites, surveys, handbooks, posters, and reports. Translation Services: Services include the translation of written, electronic and multi-media material to and from English and native foreign languages. Materials include, but are not limited to: Business, Legal, Medical, and Technical Documents. The Contractor shall provide translation services in all languages indicated in Appendices A and B as well as other languages or dialects not yet encountered by CRCL.

- Vetting: The Contractor shall also be able to provide upon request by the CRCL COR a secondary review of documents that have already been translated to validate that the translations meet the requirements of this SOW and/or to make changes or corrections where necessary to ensure the translated material accurately translates the English-language text.

4.2 Foreign Language Interpretation

CRCL requires in-person and telephonic interpretation of oral communication, on-demand or scheduled, to and from English and foreign languages in a variety of settings including but not limited to: screening and processing of individuals, interviews, reading of rights, law enforcement operations, medical screenings, communicating processes and responsibilities, presentations and discussions that may include the public, telephone hotlines, call centers, and other telephonic assistance.

The Contractor shall provide foreign language interpretation, which includes, but is not limited to: Interpreting oral communication to and from English and native foreign languages in various situations including, but not limited to,

face-to-face interview, consensual telephone conversation, live video feed, or as a third party to live conversation. Interpretation includes, but is not limited to, simultaneous, consecutive, escort, community, sight, telephonic and voiceovers.

Interpreter forums may include but are not limited to call center conversations, meetings, conferences, seminars, litigation, briefings, and training onsite or in a virtual environment. Federal or state court certifications and specialized certifications may be required. These certifications include but are not limited to medical and legal certifications.

Telephonic Interpretation: The Contractor shall provide interpreters telephonically to support calls placed by CRCL Personnel to communicate with the public or received by CRCL personnel from the public.

- 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 when requested by the CRCL COR.
- The Contractor shall provide toll free prompt access to skilled linguists
- When requested, the Contractor will ensure each interpreter be identified by a unique code that the Contractor has assigned to maintain confidentiality. The Contractor shall confirm start and end times of the call.

Sight Translation: The Contractor shall also be able to provide sight translation (translation of a written document into spoken/signed language).

The Contractor must have a back-up plan in place to address major malfunctions of its technical systems used to support telephonic interpretation without interruption. A major malfunction is a malfunction that affects the ability of the vendor to provide services to the Government. The back-up plan shall be supplied to the Government for review and approval within fifteen (15) days of contract award.

4.3 Transcription Translation/Captioning Services

CRCL requires transcription services of converting speech from audio/video sources or other format into a written or electronic text document to and from English and native foreign language. The Contractor shall provide services in all languages indicated in Appendices A and B as well as other languages or dialects not yet encountered by CRCL.

The Contractor shall provide foreign language transcription: Interprets oral communication (live or recorded) to and from English and native foreign languages and transcribe 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. Materials include but are not limited to: Business, Legal, Medical, Technical, Documents, Software, Website localization for Internet and Intranet, Video subtitling, and captioning. Include translation formatting, proofreading, text adaptation, editing, graphic design, and desktop publishing. Specialized certifications may be required (e.g. medical or legal) as needed.

4.4 Desktop Publishing Services

The Contractor will provide desktop publishing services to ensure the translated documents follow the same layout and graphic design as the English source document.

5.0 LANGUAGE SPECIALIST PERSONNEL QUALIFICATIONS

All Contractor personnel providing services under this task order shall meet the minimum qualifications and proficiency levels set forth under the DHS Language Services II BPA

6.0 QUALITY CONTROL

The Contractor must develop and maintain a Quality Control Plan (QCP) to be submitted and approved by the Government which will outline what systems and activities the Contractor will implement to ensure that all services are provided in accordance with this SOW.

- Establish an internal quality control, inspection and feedback system for all services required by the contract. Provide the means to identify deficiencies in services

- Provide 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 they will certify the proficiency of each language specialist in English and the required language.
- Methods to track timeliness and performance with respect to established standards for responsiveness and quality of service.
- Methods to measure the effectiveness of the Contractor's quality control actions.
- The QCP will also identify the individuals within the Contractor's organization with oversight authority over quality initiatives.

A draft version of the Quality Control Plan must be submitted with the Contractor's proposal.

The Contractor shall certify each translation and return said certification with the completed translation. The technical and linguistic accuracy of each translation is of paramount importance to the Government. Each translation is to be a complete, precise, 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 shall be a person other than the original translator and fluent in both the language being certified and English. The project will not be considered complete until the certification is received.

The Contractor shall complete Interpretation Certification Forms for each Interpreter assignment. The certification shall outline the date the work was performed and the hours that services were provided. The certification form shall be signed after completion of the assignment by the requestor and/or a point of contact involved with the assignment. The signed certification, along with the work order for the assignment, shall be attached to the invoice submission in order to receive payment.

7.0 CONTRACTOR PERSONNEL

The Contractor shall provide all supervisory services to support the contract such as program management, human resources management, performance management, quality assurance, and administrative support tasks. At a minimum, the Contractor shall provide the following, designated as *Key* by the Government:

Program Manager

This is a key Personnel Position: The Program Manager (PM) shall act as the central point of contact with the CRCL COR and CRCL POC for this BPA call. The PM must have at least five (5) years of experience in project management and working knowledge of various types of language services.

The PM shall ensure that CRCL has 24 hours per day, 7 days a week, and 365 days per year support and shall ensure that a Contractor representative is available with two-hour advance notice to attend any conference call requested by

the CRCL COR.

The Program Manager shall ensure all aspects of the contract are being adhered to and serve as the main point of contact for CRCL for all issues, including supervisory/management of personnel, human resource management, performance management, and quality assurance/quality improvement management.

With a minimum of two hours' notice, the Program Manager and/or representative shall be available on a daily basis for conference calls conducted by the COR and/or other representatives during the period of performance to ensure contract compliance.

In the event that the Program Manager is unavailable, an alternate Program Manager shall be designated.

7.1 Key Personnel
Before replacing any individual designated as *Key* by the Government, the Contractor shall notify the Contracting Officer and Contracting Officer's Representative no less than fifteen 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. The Contractor shall not replace *Key* Contractor personnel without acknowledgment from the Contracting Officer.

7.2 Employee Identification
Contractor employees visiting Government facilities shall wear a Government issued 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.

7.3 Employee Conduct
Contractor employees shall comply with all applicable government regulations, policies, and procedures (e.g. fire, safety, sanitation, environmental, protection, security, "off limits" areas, and possession of weapons) when visiting or working at government facilities. The Contractor shall ensure a professional appearance at all times and conduct shall not reflect discredit on the United States or the Department of Homeland Security.

7.4 Removing Employees for Misconduct or Security Reasons
The Government may, at its sole discretion, 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 this contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

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

8.0 CONFIDENTIALITY, PRIVACY, AND SECURITY CONSIDERATIONS

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.

If required by the individual task order, the Contractor shall provide information only to Homeland Security Presidential Directive 12 (HSPD-12) cleared employees, Contractors, and subcontractors having a need to know such information in the performance of their duties for this project.

The recipient certifies in writing that they will take the necessary steps to prevent the unauthorized disclosure and use of information. The Contracting Officer's Representative shall provide the prescribed non-disclosure forms as necessary to the Contractor when circumstances warrant.

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 Contracting Officer.

If public information is provided to the Contractor for use in performance or administration of this effort, the Contractor, except with the written permission of the Contracting Officer, may not use such information for any other purpose. If the Contractor is uncertain about the availability or proposed use of information provided, the Contractor will consult with the COR regarding use of that.

The Contractor agrees to assume responsibility for protecting the confidentiality of Government records which 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 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. Nothing herein shall preclude the use of any data independently acquired by the Contractor without such limitations or prohibit an agreement at no cost to the Government between the Contractor and the data owner that provides for greater rights to the Contractor.

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

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface 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 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 in order to effect compliance with such requirements.

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.

Contractor and its personnel/employees shall NOT keep any Personal Identifiable Information (PII) obtained through language services performed under this contract. 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 OMB) was, or is reasonably believed to have been, breached. Any notification shall be coordinated with DHS, and shall not proceed until DHS has made a determination that notification would not impede a law enforcement investigation 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.

9.0 EMPLOYMENT ELIGIBILITY VERIFICATION (E-Verify)

Executive Order 12989 mandates the electronic verification of all employees working on any federal contract. Each interpreter employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program, which is operated by the Department of Homeland Security in partnership with the Social Security Administration to establish work authorization.

Each language specialist working on this BPA shall be a United States citizen or an alien who has been lawfully admitted for permanent residence or other who possesses other lawful status and is authorized to work in the U.S. and possess a valid Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any subcontractor(s) and their employees.

Subject to existing law, regulations and/ or other provisions of this contract, illegal or undocumented aliens will not be employed by the Contractor, or work on this contract. The Contractor will ensure that this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this call.

SECTION III – DELIVERABLES AND ACCEPTANCE

1.0 PERIOD OF PERFORMANCE

Base Year:	September 30, 2022 – September 29, 2023
Option Year 1:	September 30, 2023 – September 29, 2024
Option Year 2:	September 30, 2024 – September 29, 2025
Option Year 3:	September 30, 2025 – September 29, 2026
Option Year 4:	September 30, 2026 – September 29, 2027

2.0 PLACE OF PERFORMANCE

The primary place of performance will be various DHS Government sites within theWashington, DC Metropolitan area.

3.0 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 7:30 AM and 4:00 PM (Eastern Time), Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW. The Government shall incur no additional costs when full-time Contractor employees definedin this SOW are required to work more than 40 hours per work week.

4.0 DELIVERABLES AND DELIVERY SCHEDULE

The contractor shall submit electronic copies of document deliverables that are indicated in the table below to the COR or the alternately designated COR back up POC via e-mail in the format specified. All document deliverables shall be made by close of business (COB) 4:30pm local time Monday through Friday, unless stated otherwise. All deliverables submitted in electronic format shall be free of any known computer virus or defects. All written reports must be submitted in electronic format with read/write capability using applications that are compatible with DHS workstations (i.e. Windows and Microsoft Office™ Applications). 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 shall be delivered in accordance with the rights set forth in FAR 52.227-17.

The deliverables that apply to this contract, and that the contractor shall provide are outlined in Table 1: Deliverables Schedule.

Table 1: Deliverables Schedule

ITEM	FREQUENCY OF DELIVERY	ACCEPTABLE FORMATS
Post Award Meeting	Within 5 business days after issuance of award	N/A
Backup Plan: Technical Malfunctions	Within 15 business days after issuance of award	Word/PDF
Final Quality Control Plan	Within 30 days after issuance of award	Word/PDF
Ad hoc reports requested by CRCL	Ad Hoc, as requested, within 24 hours	Excel or as otherwise requested

Task Order Summary Report	Monthly	Excel/Word

4.1 **Ad Hoc Reports:** The Contractor shall provide ad-hoc reports within 24 hours of the request from CRCL. See Section Deliverables.

4.2 **Task Order Summary Report:** A Microsoft Excel™ report of all task orders and upgrades placed shall be submitted on a monthly basis, or as otherwise requested by the Contracting Officer's Representative (COR) See Section 19.0 Deliverables.

4.3 **Post Award Meeting:** The Contractor shall participate in a post-award meeting with the Contracting Officer and the COR no later than five (5) business days after the date of award. The purpose of the post-award meeting is to discuss technical and contracting objectives of this contract. The post-award meeting will be held at the Government's facility or via teleconference.

5.0 Government Acceptance Period

The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are not in accordance with the terms of the task order. In the event of a rejected deliverable, the Contractor will be notified in writing by the COR of the specific reasons for rejection. The Contractor shall have an opportunity to correct the rejected deliverable.

The Contractor shall have three (3) business days to make corrections and redeliver deliverables after comments are received from the COR.

The Contractor shall be responsible for timely delivery to the COR or the alternately designated COR back-up POC. The Contractor shall work with federal personnel reviewing the deliverables to assure that the established schedule is maintained.

SECTION IV - CONTRACT ADMINISTRATION DATA

1.0 CONTRACT ADMINISTRATION

This Call Order will be administered by:

[redacted]
Contracting Officer (CO)
Office of Procurement Operations
U.S. Department of Homeland Security
[redacted]

Copies of all correspondence concerning this Call Order shall be provided to the Contracting Officer listed above.

2.0 CONTRACTING OFFICER'S REPRESENTATIVE (COR)

[redacted]
Contracting Officer's Representative
Office of Civil Rights and Civil Liberties
U.S. Department of Homeland Security (DHS)
[redacted]

3.0 CONTRACTING OFFICER'S AUTHORITY

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

SECTION V - INVOICE AND PAYMENT PROVISIONS

1.0 Invoices shall be prepared in accordance with FAR Clauses 52.232-25 Prompt Payment and 52.232-7, Payments under Time and Materials and Labor-Hours. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

a) Cover sheet identifying DHS;
b) Call Order and Associated DHS BPA Number;
c) Modification Number, if any;
d) SAM Unique Entity Identifier (UEI) Number;
e) Month services provided
f) CLIN and Accounting Classifications

2.0 Contract Line Item Number (CLIN) for each billed item shall indicate the associated CLIN and dollar amount invoiced. Supporting documentation shall include the description and monthly rate for the billing period.

3.0 The Contractor shall submit the invoices electronically to the address below:
[redacted]

4.0 Simultaneously provide an electronic copy of the invoice to the following individuals at the addresses below:

ATTN: Office of Procurement Operations/[redacted] (CO): [redacted]

ATTN: Office of Civil Rights and Civil Liberties [redacted] (COR):
[redacted]

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

SECTION VI – SPECIAL CONTRACT REQUIREMENTS

1.0 508 Compliance

Accessibility Requirements (Section 508): Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All Electronic and Information Technology (EIT) deliverables within Task Order shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards
36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS(government off-the-shelf) and COTS (commercial off-the-shelf) software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video ormultimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then 36 CFR 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functionalperformance criteria.

36 CFR 1194.41 Information Documentation and Support, applies to all documents, reports, as well as helpand support services. To ensure that documents and reports fulfill the required 36 CFR 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability totransmit and receive messages using TTY.

Section 508 Applicable Exceptions
Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply:

36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this performance work statement and for the purposes of this requirement and are not considered members of

the public.

Section 508 Compliance Requirements
36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure productswhich comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meet some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or servicesthat first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2

2.0 OTHER APPLICABLE CONDITIONS

2.1 Security

Contractor access to unclassified, but Sensitive Security Information (SSI) or Personally Identifiable Information (PII), may be required under this contract. Contractor staff members shall safeguard this information against unauthorized disclosure or dissemination. Contractor staff members are not required to have a security clearance; however, a background investigation and a suitability determination will be conducted on contractor personnel assigned to this contract.

2.1.1 Protection of Information

Contractor access to sensitive but unclassified information is required under this SOW. Contractor employees shall safeguard this information against unauthorized disclosure or dissemination in accordance with DHS MD 11042.1, Safeguarding Sensitive but Unclassified (For Official Use Only) Information. The Contractor shall ensure that all Contractor personnel having access to business or procurement-sensitive information sign a non-disclosure agreement (DHS Form 11000-6).

2.1.2 Contractor Employee Access

Sensitive Information, means any information, the loss, misuse, disclosure, or unauthorized access to or modification of which could adversely affect the national or homeland security interest, or 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:

a) 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);
b) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal
c) 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);

d) 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,

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

"Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures. The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those contractor employees authorized access to sensitive information, the contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.

The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

a) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.

b) The contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

c) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

d) Contractor access will be terminated for unauthorized use. The contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

- Non-U.S. citizens shall not be authorized to access or assist in the development, operation,

managementor maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

- The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
- There must be a compelling reason for using this individual as opposed to a U.S. citizen; and
- The waiver must be in the best interest of the Government.

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

2.1.3 Personal Identification Verification (PIV) Credential ComplianceAuthorities:

- HSPD-12 "Policies for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-06-16 "Acquisition of Products and Services for Implementation of HSPD-12"
- NIST FIPS 201 "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- NIST SP 800-63 "Electronic Authentication Guideline"
- OMB M-10-15 "FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management"

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

2.2 CONTRACTOR PERSONNEL SECURITY CLEARANCE REQUIREMENT

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

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

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

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

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

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

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

the DHS OCSO/PSD. Limited access to Government buildings is allowable without an EOD decision ifthe Contractor is escorted by a Government employee and the purpose of the visit is to attend a limited number of required briefings or nonrecurring meetings in order to facilitate the transition of a contract The intent of this statement is to allow a minimum amount of meetings/transition attendances to preparefor a new contract.

The DHS OCSO/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer's Representative (COR) all DHS issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a reportshall be submitted to the COR, referencing the pass or card number, name of individual to whom it wasissued 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 sensitivedata being processed. Contractor personnel must have a favorable Entry on Duty or fitness determination by the DHS Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD), to access this information.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civilpenalties and sanctions under a variety of laws (e.g., Privacy Act).

2.3 SECURITY OFFICE CONTACT

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

SECTION VII – CONTRACT CLAUSES

All contract clauses from the Contractor's Language Services II Blanket Purchase Agreement (BPA) will be incorporated into this BPA Call.

The following contract clauses and provisions are incorporated in full text:

52.217-8 Option to Extend Services (Nov 1999)
The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 14 months. The Contracting Officer may exercise the option by written notice to the Contractor within **30 days**.

(End of clause)

52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment. (Aug 2020)

(a) Definitions. As used in this clause—

Backhaul means intermediate links between the core network, or backbone network, and the small subnetworks at the edge of the network (e.g., connecting cell phones/towers to the core telephone network). Backhaul can be wireless (e.g., microwave) or wired (e.g., fiber optic, coaxial cable, Ethernet).

Covered foreign country means The People's Republic of China.

Covered telecommunications equipment or services means–

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2) For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3) Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology means–

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export

Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

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

Reasonable inquiry means an inquiry designed to uncover any information in the entity's possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.

Roaming means cellular communications services (e.g., voice, video, data) received from a visited network when unable to connect to the facilities of the home network either because signal coverage is too weak or because traffic is too high.

Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.

(b) Prohibition. (1) Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104.

(2) Section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2020, from entering into a contract, or extending or renewing a contract, with an entity that uses any equipment, system, or service that uses

covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in FAR 4.2104. This prohibition applies to the use of covered telecommunications equipment or services, regardless of whether that use is in performance of work under a Federal contract.

(c) Exceptions. This clause does not prohibit contractors from providing—

(1) A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2) Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d) Reporting requirement. (1) In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i) Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e) and excluding paragraph (b)(2), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

(End of clause)

3052.204-70 SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or

electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the Quoter's Quotation. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

(3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

(c) Examples of tasks that require security provisions include--

(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and

(2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).

(d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 13.1, July 27, 2017) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

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.

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 tobe kept secret in the interest of national defense, homeland security or foreign policy. This definition includesthe 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 Sensitive Systems Policy Directive 4300A
(3) DHS 4300A Sensitive Systems Handbook and Attachments
(4) DHS Security Authorization Process Guide
(5) DHS Handbook for Safeguarding Sensitive Personally Identifiable Information
(6) DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program
(7) DHS Information Security Performance Plan (current fiscal year)
(8) DHS Privacy Incident Handling Guidance
(9) Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules accessible at http://csrc.nist.gov/groups/STM/cmvp/standards.html
(10) 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
(11) 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* and the *DHS 4300A Sensitive Systems Handbook* provide the policies and procedures on security for Information Technology (IT) resources. The *DHS Handbook for Safeguarding Sensitive Personally Identifiable Information* provides guidelines to help safeguard SPII in both paper and electronic form. *DHS Instruction Handbook 121-01-007 Department of Homeland Security Personnel Suitability and Security Program* establishes procedures, program responsibilities, minimum standards, and reporting protocols for the DHS Personnel Suitability and Security Program.

(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 Sensitive Systems Policy Directive 4300A* (Version 11.0, April 30, 2014), or any successor publication, *DHS 4300A Sensitive Systems Handbook* (Version 9.1, July 24, 2012), or any successor publication, and the *Security Authorization Process Guide* including templates.

(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 Contractorshall 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 Handbook Incident Response and Reporting* requirements. 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 Contracting Officer 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 Contractor has 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 Sensitive Systems Handbook Incident Response and Reporting*, 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*.

SECTION X – APPENDICES AND ATTACHMENTS

Appendix A: List of Languages – Translation and Interpreter Services
Appendix B: List of Language Previous Encountered – Interpretation
Appendix C: Examples of Uncommon and Rare Languages and Dialects

Appendix A
List of Languages – Translation and Interpreter Services

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

Legend

Linguae Requested Most Often | *Language Requested Least Often*

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

Appendix B
List of Language Previous 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

Linguae Requested Most Often | *Language Requested Least Often*

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

Appendix B
List of Language Previous Encountered – Interpretation (Cont'd)

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

Legend

Linguae Requested Most Often | *Language Requested Least Often*

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