# DEPARTMENT OF HOMELAND SECURITY (DHS)

# STATEMENT OF WORK (SOW)
# FOR
# EEO COUNSELING AND EEO INVESTIGATION SERVICES

## 1.0 GENERAL

### 1.1 BACKGROUND

CISA's mission is to lead the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure. CISA includes the CISA Mission Enabling Offices (MEOs) and six Divisions: the Cybersecurity Division (CSD), the Emergency Communications Division (ECD), the Integrated Operations Division (IOD), Infrastructure Security Division (ISD), the Stakeholder Engagement Division (SED), as well as, the National Risk Management Center (NRMC), which are headquartered with the National Capital Region (NCR).

The mission of the Office of Equity, Diversity, Inclusion and Accessibility (OEDIA) at the Cybersecurity and Infrastructure Security Agency (CISA) is to cultivate an inclusive culture that champions dignity, respect, and belonging where diverse talent is leveraged equitably to advance cybersecurity and infrastructure security by promoting Equal Employment Opportunity (EEO) through elimination and prevention of unlawful discrimination. OEDIA enforce laws, regulations, executive orders, and policies which prohibit unlawful discrimination in employment on the basis of race, color, religion, national origin, age, disability, sex, sexual orientation, parental status, and protected genetic information.

OEDIA enforce laws, regulations, Executive Orders, and policies which prohibit retaliation for opposing any practice made unlawful by Title VII of the Civil Rights Act of 1964, as amended; the Age Discrimination in Employment Act (ADEA), as amended; the Equal Pay Act, the Rehabilitation Act, as amended; and the Genetic Information Nondiscrimination Act (GINA), or for participating in any stage of administrative or judicial proceedings under those statutes.

OEDIA reports directly to the Deputy Director of CISA and is responsible for the overall management, administration, and oversight of the CISA EEO programs, including, but not limited to Affirmative Employment Programs, Reasonable Accommodations, Selective Placement, Disabled Veterans, EEO Training, Alternative Dispute Resolution (ADR), and EEO Complaint Processing.

### 1.2 SCOPE

The purpose of this task order is to acquire EEO Counseling and Investigative Support services for CRCL/OEDIA. The services may relate to EEO informal and formal complaints arising from one of the organizational subdivisions at CISA or relate to EEO complaints arising in another DHS Component, which is processing because it would pose a conflict of interest in the originating Component. All services will be performed in accordance with the Equal Employment Opportunity Commission (EEOC) Regulations set forth at 29 C.F.R. Part 1614, EEOC Management Directive (MD) 110, EEOC caselaw precedents, and any subsequent law, statute, regulation, or directive that may apply.

### 1.3 REFERENCES

The following references are pertinent to the services performed for this requirement:

- DHS Form 3090-1, Individual Complaint of Discrimination

- 29 C.F.R. § 1614
- EEOC's Management Directive-110
- Title VII of the Civil Rights Act of 1964 (Title VII), 42 U.S.C. §§ 2000(e) - 2000(e-17)
- Section 501 of the Rehabilitation Act of 1973 (Rehabilitation Act), 29 U.S.C. § 791.
- The Age Discrimination in Employment Act of 1967 (ADEA), 29 U.S.C. §§ 621-634 (2015)
- The Equal Pay Act of 1963 (EPA), 29 U.S.C. § 206 (d)(1)
- The Genetic Information Nondiscrimination Act of 2008 (GINA), 42 U.S.C. §§2000(ff)-2000(ff- 11)

## 2.0 SPECIFIC REQUIREMENTS/TASKS

### 2.1 TASK ONE. *EEO COUNSELING SERVICES*

The Contractor shall provide 30 counseling cases plus 20 optional cases to individual agency employees, applicants for employment, and contractor support staff who believe they have been discriminated against on the basis of race, color, national origin, religion, sex (including sexual orientation, gender identity, pregnancy), age, physical or mental disability, retaliation/reprisal, parental status, and protected genetic information. The Contractor will perform the following EEO counseling services:

2.1.1 Schedule initial counseling session and inform their right to reasonable accommodations.

2.1.2 Advise individuals of their rights and responsibilities in the Federal sector EEO complaint process, in accordance with 29 C.F.R. § 1614.105(b).

2.1.3 Inform individuals that they can participate in the Alternative Dispute Resolution (ADR) program or Traditional EEO Counseling. The counselor will fully explain the Agency's ADR Program. The counselor will provide, in writing, the requirements for initiating a formal EEO complaint, if the dispute is not resolved through counseling or ADR.

2.1.4 Identify whether the aggrieved individual is the applicant, current or former Federal employee, or a contractor along with position title, organizational subdivision, and preferred contact information.

2.1.5 Determine whether the aggrieved individual is represented by an attorney or non-attorney representative. If the former, direct all future correspondence through the attorney and copy the aggrieved individual.

2.1.6 Seek consent for electronic transmittal of EEO correspondence aggrieved individuals and their representatives as permitted under EEOC caselaw.

2.1.7 Identify and articulate each claim (alleged injury to aggrieved) without fragmentation, basis(es) of each claim, alleged discriminating individuals, and applicable legal theory(ies) being raised in the pre-compliant.

2.1.8 Conduct thorough inquiry and gather documentation necessary to make reasoned jurisdictional determination under 29 C.F.R. § 1614.107, including but not limited to:

- Date of initial EEO contact, initial interview, and final interview.
- Date of most recent alleged discriminatory incident, date(s) of each claim involving a discrete act, EEO training records, and reasons for delayed EEO contact for each discrete act where applicable.
- Whether same claim(s) have been also raised before a negotiated grievance procedure, Merit Systems Protection Board (MSPB), or US District Court and include relevant filings and documentation.
- Written notice of potential dismissal for failure to respond to requests for information within business 15 days where applicable.
- Evidence of the date of receipt/delivery of all requisite notices and EEO correspondence conspicuously verifying the transmittal(s) was made to the correct (electronic) address as designated by the aggrieved individual and their representatives as prescribed by EEOC caselaw.

2.1.9 Facilitate shuttle diplomacy with the consent of the aggrieved individual and management to encourage resolution of the matter at the lowest level possible.

2.1.10 Conduct final interview at least seven (7) calendar days prior to the regulatory 30-day deadline unless an extension is agreed upon by the aggrieved individual and OEDIA. If the latter, it must be completed seven (7) calendar days prior to the extended deadline (up to the regulatory 90-day limit).

2.1.11 Document successful resolutions, or provide aggrieved individuals written Notice of Right to File a formal complaint (NRTF) within the applicable 30–90-day timeframe as prescribed by 29 C.F.R. § 1614.105(d)-(e). In the latter case, the Contractor will obtain sufficient documentary evidence to establish the date of receipt by the aggrieved individual and their representatives as prescribed under EEOC caselaw (e.g., email acknowledgment or electronic tracker establishing when the file was access of file by the aggrieved individual).

2.1.12 Provide the Counselor's Report to the aggrieved individual together with the issuance of the NRTF, unless an extension is granted by the EEO Complaints Program Manager. If an extension is granted, provide a statement claim(s) to the aggrieved individual together with the issuance of the NRTF and the Counselor's Report within five (5) calendar days thereafter.

2.1.13 Obtain the aggrieved individual's written agreement of the claims and basis(es) as framed.

2.1.14 Meet all regulatory timeframes outlined in 29 C.F.R. Part 1614 of EEOC's regulations

### 2.2 TASK TWO. *EEO INVESTIGATIVE SERVICES*

The Contractor shall provide the following 30 plus 20 optional EEO investigation services:

2.2.1 Develop an impartial and appropriate factual record upon which to make findings on claims raised by the complainant(s). An appropriate factual record is one that allows a reasonable fact finder to draw conclusions as to whether discrimination occurred.

2.2.2 Arrange and conduct interviews with the complainant(s), witnesses, and management officials relative to the complaint. If the complainant is represented by an attorney, the investigator's contact will be with the attorney unless the complainant and attorney agree that the complainant can be contacted directly. OEDIA will provide

guidance to the Contractor as to whether the complaint will be investigated as an individual case or as a consolidated case.

2.2.3 Secure affidavits from complainant(s), management official(s), and witness(es) produced from responsive answers to interrogatories or interview questions (on-site or telephonic interviews).

2.2.4 Ask the complainant(s) to identify the basis for each claim (race, sex, age, etc.), to describe the treatment complained of, and to identify others who received more favorable treatment or detail what other factual reasons for their belief that they were discriminated against.

2.2.5 Provide the complainant(s) the opportunity to define a claim for compensatory damages and to set out fully how they were injured-in-fact, what relief is requested, and the nature of that relief.

2.2.6 Ask the complainant(s) to identify witnesses who otherwise have personal direct first-hand knowledge of the matter(s) giving rise to the complaint. Ask the complainant(s) to explain what direct first-hand knowledge each witness can testify to and provide their contact information.

2.2.7 Require management officials who were involved in the decision-making process to explain their rationale for each action raised in the complaint. Seek documentary evidence

2.2.8 Provide the complainant(s) with the opportunity to rebut management's reasons for each claim under investigation.

2.2.9 Expend reasonable efforts to identify and seek testimony from other witnesses with personal direct first-hand knowledge of the matters raised in the complaint.

2.2.10 Request and gather relevant documentation such as statistical, personnel records, comparative data, and objective evidence (e.g., medical records that would verify injury or harm).

2.2.11 Alert the EEO Complaints Program Manager and Chief, OEDIA in absence of EEO Complaints Manager of additional claims raised by complainant(s) and seek approval prior to expanding the scope of the investigation.
2.2.12 Ensure that all regulatory timeframes outlined in 29 C.F.R. Part 1614 of EEOC's requirements are met.

**3.0 GOVERNMENT ACCEPTANCE PERIOD**
The COR will review deliverables prior to acceptance and provide the contractor with an e-mail that provides documented reasons for non-acceptance. If the deliverable is acceptable, the COR will send an e-mail to the Contractor notifying it that the deliverable has been accepted.

3.1 The COR will have the right to reject or require correction of any deficiencies found in the deliverables that are contrary to the information contained in the Contractor's accepted proposal. 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 may have an opportunity to correct the rejected deliverable and return it per delivery instructions.

3.2 The COR will have 5 business days to review deliverables and make comments. The Contractor shall have 5 business days to make corrections and redeliver.

3.3 All other review times and schedules for deliverables shall be agreed upon by the parties based on the final approved Project Plan. The Contractor shall be responsible for timely delivery to Government personnel in the agreed upon review chain, at each stage of the review. The Contractor shall work with personnel reviewing the deliverables to assure that the established schedule is maintained.

## 4.0 DELIVERABLES

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

| ITEM | SOW REFERENCE | DELIVERABLE / EVENT | DUE BY | DISTRIBUTION |
|---|---|---|---|---|
| 1 | 6.3 | **Post Award Conference** | Within five (5) business days of task order award or as coordinated by the CO/CS | In person meeting or by conference call |
| 2 | 6.3 | Draft Contractor Project Plan | Presented at kick-off meeting | COR, Contracting Officer |
| 3 | 6.4 | **Final Contractor Project Plan** | Five (5) business days after kick-off meeting | COR, Contracting Officer |
| 4 | 6.5 | **Progress Reports** | 4:00 PM EST every Monday beginning after date of award | COR, Assigned OEDIA POC |
| 5 | 6.6.1 | **Draft EEO Counselor Reports** | Three (3) calendar days after conducting final interview | COR, Assigned OEDIA POC |
| 6 | 6.6.1 | Final EEO Counselor Reports | Two (2) calendar days after Government approval of draft together with NRTF | COR, Assigned OEDIA POC |
| 7 | 6.6.2 | Draft Investigative (IP) & Document Request (DR) | Five (5) business days after assignment of the case | COR, Assigned OEDIA POC |
| 8 | 6.6.2 | Proposed Report of Investigation (ROI) | Forty-Five (45) calendar days after assignment of the case | COR, Assigned OEDIA POC |

| ITEM | SOW REFERENCE | DELIVERABLE / EVENT | DUE BY | DISTRIBUTION |
|---|---|---|---|---|
| 9 | 6.6.2 | Revised Reports of Investigation (ROI) | Ten (10) calendar days after Government approval of the draft ROI summary | COR, Assigned OEDIA POC |

## 5.0 CONTRACTOR PERSONNEL

### 5.1 Qualified Personnel

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

5.1.1 All contract counselors and investigators shall possess the required training as outlined in EEOC Management Directive 110. Investigators shall have at least five (5) years of investigative experience.

5.1.2 Contractor personnel shall have excellent writing skills, superior factual and analytical ability, ability to work with minimal supervision, and professional objectivity. Experience may be gained as a federal employee, a contractor supporting a federal agency, an intern assigned to a federal agency, or in any other position requiring detailed knowledge and understanding of 29 C.F.R. § 1614.101 et seq.

5.1.3 The Contractor shall ensure that contractor personnel remain abreast of statutory, regulatory, and case law developments arising under relevant employment statutes by providing specialized training and/or technical assistance opportunities to contractor staff members at least annually through attendance at EEOC Training Institute presentations or similar instructional opportunities

### 5.2 Continuity of Support

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

### 5.3 Key Personnel

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

**5.3.1** Contractor *Key* personnel shall not be assigned by the Contractor to more than one key position for this requirement.

### 5.4 Project Manager

The Contractor shall provide a Project Manager who shall be responsible for all Contractor work performed under this SOW. The Project Manager shall be a single point of contact for the Contracting Officer and the COR. It is anticipated that the Project Manager shall be one of the senior level employees provided by the Contractor for this work effort. The name of the Project Manager, and the name(s) of any alternate(s) who shall act for the Contractor in the absence of the Project Manager, shall be provided to the Government as part of the Contractor's proposal. The Project Manager is further designated as *Key* by the Government. During any absence of the Project Manager, only one alternate shall have full authority to act for the Contractor on all matters relating to work performed under this contract. The Project Manager and all designated alternates shall be able to read, write, speak and understand English. Additionally, the Contractor shall not replace the Project Manager without prior approval from the Contracting Officer.

**5.4.1** The Project Manager shall be available to the COR via telephone between the hours of 9:30a.m. and 6:30 p.m. EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within two (2) hours of notification.

### 5.5 Employee Identification

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

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

### 5.6 Employee Conduct

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

### 5.7 Removing Employees for Misconduct or Security Reasons

The Government may, at its sole discretion (via the Contracting Officer), direct the Contractor to remove any Contractor employee from DHS facilities for misconduct or security reasons. Removal does not relieve the Contractor of the responsibility to continue providing the services

required under the contract. The Contracting Officer will provide the Contractor with a written explanation to support any request to remove an employee.

## 6.0 OTHER APPLICABLE CONDITIONS

### 6.1 PERIOD OF PERFORMANCE

The period of performance for this contract is a one-year base period with two one-year option periods as follows:

| | |
|---|---|
| Base Period | September 30, 2023 through September 29, 2024 |
| Option Period One | September 30, 2024 through September 29, 2025 |
| Option Period Two | September 30, 2025 through September 29, 2026 |

### 6.2 PLACE OF PERFORMANCE

The place of performance for work performed under this task order will be at the Contractor's site or Contractor's remote location.

### 6.3 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference 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 Conference, which will be chaired by the Contracting Officer, is to discuss technical and contracting objectives of this contract and review the Contractor's draft project plan. The Post Award Conference will be held via teleconference.

### 6.4 PROJECT PLAN

The Contractor shall provide a draft Project Plan at the Post Award Conference for Government review and comment. The Contractor shall provide a final Project Plan to the COR not later than five (5) business days after the Post Award Conference.

### 6.5 PROGRESS REPORTS

The Project Manager shall provide a weekly progress report 4:00 PM EST every Monday beginning after date of award to the Contracting Officer and COR via electronic mail. This report shall include a summary of all Contractor work performed, including a breakdown of labor hours by labor category, all direct costs by line item, an assessment of technical progress, schedule status, any travel conducted and any Contractor concerns or recommendations for the previous reporting period.

### 6.6 GENERAL REPORT REQUIREMENTS

The Contractor shall provide all written reports in electronic format with read/write capability using applications that are compatible with DHS workstations (Windows XP and Microsoft Office Applications).

The Contractor shall provide the reports listed below, including all data and analysis created as required.

#### 6.6.1 EEO Counselor Reports

The Contractor shall provide an EEO counselor reports, as outlined in 29 C.F.R. § 1614 and the EEOC's Management Directive -110, for each EEO counseling case performed. The report will include a chronology of counseling activity. It will articulate the nature of the matters raised during counseling and frame the basis(es) of alleged discrimination; applicable legal theory(ies); claim(s) of injury inclusive of dates for each discrete act and alleged discriminating individuals (if

known); and the remedies requested. It will provide a recitation of relevant facts., management response to matters raised, attempts to resolve the complaint, and all other relevant information and documents prescribed here in § 3.2 and Appendix I.

A draft report will be provided in a Microsoft Word (docx) compatible format, within three (3) calendar days following the final interview with the aggrieved individual. Upon the Government's approval, the Contractor will securely transmit the final EEO counselor's report in an accessible (508 compliant) portable document format (PDF) within two (2) calendar days. The PDF file will provide Bates numbering, bookmarks for each section of the report with nested bookmarks for each individually distinguishable documents within its attachments and have full optical character recognition (OCR) completed.

### 6.6.2 EEO Investigator Reports

The Contractor shall provide a report of investigations (ROI), as outlined in 29 C.F.R. § 1614 and the EEOC's Management Directive-110, for each case of investigations performed. A draft documents request (DR) and investigative plan (IP) of interrogatories for complainant, management official(s), and witnesses shall be provided via electronic media in a Microsoft Word (docx) compatible format, within five (5) business days from the assignment of the EEO case, unless an extension is granted by the EEO Complaints Program Manager. The IP will include the statement of accepted claims, identify applicable legal theories, issues, and standard of proof. The IP will note the investigative methods to be used and expected timeline for the investigation. The DR should articulate description of potentially probative documentary, identify their sources, personnel records, workforce data, and/or comparative statistical evidence. Contract investigators must establish deadlines for receipt of information. If the appropriate parties fail to timely comply, investigators document the attempt in the ROI. Contract investigators shall share each affidavit when they are obtained with the EEO Complaints Program Manager.

A completed draft of the ROI detailing the results of the EEO investigation, including all exhibits, shall be provided via secure electronic portal in a (508 compliant) PDF format within forty-five (45) calendar days from the assignment of the EEO case, unless an extension is granted by the EEO Complaints Program Manager. The draft index/summary must also be submitted in Microsoft Word compatible (docx.) format electronically. Upon the Government's approval of the draft ROI report, the Contractor shall provide the final ROI in an accessible (508 compliant) PDF, via a secure online portal, within five (5) calendar days. The PDF file shall be consistent with the requirements set forth in EEOC Management Directive 110, Chapter 6 § VIII, and provide Bates numbering on each page, bookmarks for each major section of the report as well as nested bookmarks for all individually distinguishable documents within exhibits and have full optical character recognition (OCR) completed. The index/summary must also be submitted in Microsoft Word compatible (docx.) format electronically.

## 6.7 INTELLECTUAL PROPERTY

All Contractor developed processes and procedures and other forms of intellectual property first developed under this task order shall be considered Government property.

All documentation, electronic data, and information collected by the Contractor and entered into a database or generated shall be considered Government property and shall be returned to the Government at the end of the performance period.

### 6.8 PROTECTION OF INFORMATION

Complaint files contain personal data that shall be treated in a confidential manner. Contractor use is restricted to contractor personnel directly involved in preparing or reviewing the deliverables described in this task order. Material from complaint files transmitted electronically from the Contractor to the Government (as well as such transmissions between Contractor personnel) shall be encrypted and password protected, with password identification transmitted by separate communication, except that are documents uploaded to a secure online portal do not require password protection. Generally, the Government will not need to provide the Contractor with any printed materials from a complaint file, and the Contractor will not need to produce any printed materials from a complaint file. However, in the unusual case in which it is necessary for the Contractor to possess printed material from a complaint file, such documents shall be stored in a locked cabinet or secure area

## 7.0 RECORDS MANAGEMENT OBLIGATIONS

**7.1.1** Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chs. 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

**7.1.2** In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

**7.1.3** In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Electronic records and associated metadata must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

**7.1.4** CISA and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of CISA or destroyed except for in accordance with the provisions of the agency records schedules and with the written concurrence of the Head of the Contracting Activity. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must report to CISA. The agency must report promptly to NARA in accordance with 36 CFR 1230.

**7.1.5** The Contractor shall immediately notify the appropriate Contracting Officer upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the GSA Schedule. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly protected. The Contractor shall not remove

material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to CISA control or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand carried, mailed, emailed, or securely electronically transmitted to the Contracting Officer or address prescribed in the GSA Schedue. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

**7.1.6** The Contractor is required to obtain the Contracting Officer's approval prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and CISA guidance for protecting sensitive, proprietary information, classified, and controlled unclassified information.

**7.1.7** The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with CISA policy.

**7.1.8** The Contractor shall not create or maintain any records containing any non-public CISA information that are not specifically tied to or authorized by the contract.

**7.1.9** The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

**7.1.10** CISA owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which CISA shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

**7.1.11** Training

All Contractor employees assigned to this contract who create, work with, or otherwise handle records are required to take CISA-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

**7.1.12** Flowdown of requirements to subcontractors

The Contractor shall incorporate the substance of this clause, its terms and requirements including this paragraph, in all subcontracts under this [contract vehicle], and require written subcontractor acknowledgment of same. Violation by a subcontractor of any provision set forth in this clause will be attributed to the Contractor.

## 8.0 SECTION 508 COMPLIANCE

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public

with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

All products, platforms and services delivered as part of this work statement that, by definition, are deemed ICT shall conform to the revised regulatory implementation of Section 508 Standards, which are located at 36 C.F.R. § 1194.1 & Appendixes A, C & D, and available at https://www.ecfr.gov/cgi-bin/text-idx?SID=e1c6735e25593339a9db63534259d8ec&mc=true&node=pt36.3.1194&rgn=div5. In the revised regulation, ICT replaced the term electronic and information technology (EIT) used in the original 508 standards. ICT includes IT and other equipment.

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 Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018 and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

### 8.1 Section 508 Requirements for Technology Services

- When developing or modifying ICT, the Contractor is required to validate ICT deliverables for conformance to the applicable Section 508 requirements. Validation shall occur on a frequency that ensures Section 508 requirements is evaluated within each iteration and release that contains user interface functionality.
- When modifying, installing, configuring or integrating commercially available or government-owned ICT, the Contractor shall not reduce the original ICT Item's level of Section 508 conformance.
- When developing or modifying electronic documents and forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable to the applicable Section 508 standards (including WCAG Level A and AA Level 2.0 Success Criteria) by conducting testing using the test methods published under "Accessibility Tests for Documents" at https://www.dhs.gov/compliance-test-processes.
- Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

### 8.2 Section 508 Deliverables

- **Section 508 Test Plans**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide a detailed Section 508 Conformance Test Plan. The Test Plan shall describe the scope of components that will be tested, an explanation of the test process that will be used, when testing will be conducted during the project development life cycle, who will conduct the testing, how test results will be reported, and any key assumptions.
- **Section 508 Test Results**: When developing or modifying ICT pursuant to this contract, the Contractor shall provide test results in accordance with the Section 508 Requirements for Technology Services provided in this solicitation.

- **Section 508 Accessibility Conformance Reports**: For each ICT item offered through this contract (including commercially available products, and solutions consisting of ICT that are developed or modified pursuant to this contract), the Offeror shall provide an Accessibility Conformance Report (ACR) to document conformance claims against the applicable Section 508 standards. The ACR shall be based on the Voluntary Product Accessibility Template Version 2.0 508 (or successor versions). The template can be found at https://www.itic.org/policy/accessibility/vpat. Each ACR shall be completed by following all of the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.
- **Other Section 508 Documentation:** The following documentation shall be provided upon request for ICT items offered through this contract:
    - Documentation of features provided to help achieve accessibility and usability for people with disabilities.
    - Documentation on how to configure and install the ICT Item to support accessibility.
    - Documentation of core functions that cannot be accessed by persons with disabilities.
    - Documentation of remediation plans to address non-conformance to the Section 508 standards

## 9.0 GOVERNMENT TERMS & DEFINITIONS

a) DHS – U.S. Department of Homeland Security
b) CRCL - Office for Civil Rights and Civil Liberties
c) CO – Contracting Officer
d) COR – Contracting Officer's Representative
e) PM - Project Manager
f) Title VII - Title VII of the Civil Rights Act of 1964, as amended
g) ADEA - Age Discrimination in Employment Act
h) ADA Amendments Act – ADA Amendments Act of 2008
i) GINA – Genetic Information Nondiscrimination Act of 2008
j) CFR - Code of Federal Regulations
k) EEO - Equal Employment Opportunity
l) EEOC - Equal Employment Opportunity Commission
m) 29 C.F.R. §1614.101 et seq. - Title 29, Code of Federal Regulations Part 1614
n) EEOC Management Directive 110 (MD-110)

## 10.0 GOVERNMENT FURNISHED RESOURCES

The Government will provide contractor personnel with the applicable documents, electronically in most cases, pertaining to the complaint. For EEO counseling services, these documents will include any intake documents. For EEO investigative services, these documents will include intake documents, the counselor's report, the formal complaint, the acknowledgment letter, the acceptance letter, and a letter of authority.

## 11.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract, except for the Government Furnished Resources specified in SOW 16.0.

## 12.0 INVOICES AND PAYMENT PROVISIONS

Invoices shall be prepared per Section VII, Contract Clauses; Paragraph A. entitled "FAR CLAUSES INCORPORATED BY REFERENCE," FAR Clause 52.232-25 Prompt Payment, addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1) Cover sheet identifying DHS;
2) Task Order Number;
3) Modification Number, if any;
4) UEI Number;
5) Month services provided
6) CLIN and Accounting Classifications
7) Contract Line Item Number (CLIN) and description for each billed item.
8) Any additional backup information as required by this contract.
9) ATTN: CISA/OEDIA

The contractor shall submit invoices monthly. The Contractor shall submit the invoice electronically to the address below:

[redacted]

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

[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.

## 13.0 DHS IT SECURITY LANGUAGE

DHS 4300A Ver.13.1 Contractors and Outsourced Operations

- DHS 4300A Policy 3.3.a. - All Statements of Work (SOW) and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.

- DHS 4300A Policy 3.3.b. - All Contractor information system services and operations shall adhere to all applicable DHS information security policies.

- DHS 4300A Policy 3.3.c. - Requirements shall address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems. Requirements shall also include requirements for personnel background I investigations and clearances, and facility security.

- DHS 4300A Policy 3.3.d. SOWs and contracts shall include a provision stating that, when the contract ends, the contractor shall return all information and information resources provided during the life of the contract and certify that all DHS information has been purged from any contractor-owned system(s) that have been used to process DHS information.

- DHS 4300A Policy 3.3.e. - Components shall conduct reviews to ensure that information security requirements are included in contract language and that the requirements are met throughout the life of the contract.

DHS 4300A Ver.13.1 3.12 Information Security Policy Violation and Disciplinary Action

- Individual accountability is a cornerstone of an effective security policy. Component Heads are responsible for taking corrective actions whenever security incidents or violations occur and for holding personnel accountable for intentional violations. Each Component must determine how to best address each individual case.

- DHS 4300A Policy 3.12.a - Violations related to information security are addressed in Standards of Ethical Conduct for Employees of the Executive Branch; DHS employees may be subject to disciplinary action for failure to comply with DHS security policy whether or not the failure results in criminal prosecution.

- DHS 4300A Policy 3.12.b. - Non-DHS Federal employees, contractors, or others working on behalf of DHS who fail to comply with Department security policies are subject to termination of their access to DHS systems and facilities whether or not the failure results in criminal prosecution.

- DHS 4300A Policy 3.12.c - Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.

DHS 4300A Ver. 13.1 4.1.2 Rules of Behavior

- DHS 4300A Policy 4.1.2.a - Components shall ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a "Consent to Monitor" provision) and that disciplinary actions may result from violations.

- DHS 4300A Policy 4.1.2.b - Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.

DHS 4300A Ver.13.1 4.1.5 Information Security and Privacy Awareness, Training, and Education

- DHS 4300A Policy 4.1.5.a - Components shall establish an information security training program for users of DHS information systems.

- DHS 4300A Policy 4.1.5.b - DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) accessing DHS systems shall receive initial training and annual refresher training in security awareness and accepted security practices. Personnel shall complete security awareness training within twenty-four (24) hours of being granted a user account. If a user fails to meet this training requirement, user access shall be suspended.

- DHS 4300A Policy 4.1.5.c - DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) with significant security responsibilities (e.g., Information Systems Security Officers (ISSO), system administrators) shall receive initial specialized training and thereafter annual refresher training specific to their security responsibilities.

DHS 4300A Ver.13.1 4.2.1 General Physical Access

- DHS 4300A Policy 4.2.1.d - Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.

DHS 4300A Ver.13. 1 4.3.1 Media Protection

- DHS 4300A Policy 4.3.1.c - DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government-issued removable media (USB

drives and from connecting them to DHS equipment or networks or using them to store DHS sensitive information.

DHS 4300A Ver.13. 1 4.8.5 Personal Use of Government Office Equipment and DHS Systems/Computers

- DHS 4300A Policy 4.8.5.c - Anyone granted user account access to any DHS information system (including DHS employees, contractors, and others working on behalf of DHS) shall have no expectations of privacy associated with its use. By completing the authentication process, the user acknowledges his or her consent to monitoring.