DEPARTMENT OF HOMELAND SECURITY (DHS)

STATEMENT OF WORK (SOW)
FOR
Barrier Analysis

<Contracting Officer enter final date solicitation is released>

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 enforces 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, reprisal, parental status, and protected genetic information.

The EEOC's Management Directive 715 (MD-715) provides guidance on creating and maintaining a model Equal Employment Opportunity (EEO) Program. To comply with MD-715 and 29 CFR 1614.102(a)(3), CISA is obligated to conduct a continuing campaign to eradicate every form of prejudice or discrimination from personnel policies, practices, and working conditions, identify areas where barriers may operate to exclude certain groups, and develop plans to eliminate identified impediments to equal opportunity through conducting barrier analyses. The primary purpose of the final reports will be the identification and analysis of potential barriers to equal employment opportunities within the CISA applicant, hiring and retention processes, such as promotions and training, and to obtain cogent solutions for resolving any found to exist.

The MD-715 requires federal agencies to identify barriers which may inhibit free and open workplace competition and develop meaningful plans to eliminate those barriers. The barrier analysis process requires examination of agency policies, procedures and practices to uncover barriers to equal employment opportunity. Once the barriers have been identified, agencies are required to eliminate the barriers or mitigate the impact.

1.2 SCOPE

The CISA requires consulting services to support the CISA's OEDIA. The contractor shall work directly with CISA staff, with direct consultation from the Contracting Officer's Representative (COR), to ensure that a quantitative and qualitative analysis of hirings, promotions, and leadership training (Barrier Analysis) is completed in compliance with Equal Employment Opportunity Commission (EEOC) Management Directive 715 (MD-715).

1.3 OBJECTIVE

The CISA seeks to procure the services of a qualified contractor who can assist in carrying out and reporting on all aspects of the barrier analysis research process, as specified in the U.S. Equal Employment Opportunity Commission (EEOC)'s Management Directive 715 (MD-715) and accompanying instructions (as updated) and all related or relevant EEOC and legal guidance, as well as other related tasks specified in the Task Areas section.

The CISA's approach to Equal Employment Opportunity is that it is a shared responsibility among all Divisions, Offices, and personnel. The barrier analysis, reporting, and ad-hoc analytic consultation must be rigorous enough to withstand critique from highly informed subject matter experts and executives. Our program goes beyond simple trigger analysis of proportions that drive the MD- 715 Report to using social science research methods that give our conclusions a high level of credibility and give our organization the confidence that our recommendations are going to work. To that end, the CISA seeks to procure contract talent on barrier analysis that is highly skilled and has the potential to be industry leading. We seek to procure significant expertise in both social science and in personnel management, which are critical to securing the coordination we need across the agency and support for our recommendations from upper management.

The barrier analyses must establish the connection between the statistical outcomes observed in employment phases and specific causes in practice and procedure, as well the connection between those causes and recommendations. Procuring teams that have the proper training, experience, and a high level of availability among key personnel is the first priority to ensure these outcomes are achieved effectively.

1.4 APPLICABLE DOCUMENTS

1.4.1 Compliance Documents

The following documents provide specifications, standards, or guidelines that must be complied with in order to meet the requirements of this contract:

- 29.CFR 1614, MD-715 guidance
- Title VII of the Civil Rights Act of 1964
- Pregnancy Discrimination Act of 1978
- The Age Discrimination in Employment Act of 1967 (ADEA)
- Genetic Information Non-discrimination Act of 2008 (GINA)
- Sections 102 and 103 of the Civil Rights Act of 1991
- The Equal Pay Act of 1963 (EPA)
- Rehabilitation Act of 1973
- The Americans with Disabilities Act Amendments Act of 2008
- Sections 501 and 505 of the Rehabilitation Act of 1973
- Pregancy Workers Fairness Act of 2023
- Title 29 CFR, Part 1614 (Federal Sector Equal Employment Opportunity)
- Title 29 CFR, Part 1607 (Uniform Guidelines on Employee Selection Procedures)

1.4.2 Reference Documents

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

- 29 CFR §1614
- EEOC MD-715 guidance

2.0 SPECIFIC REQUIREMENTS/TASKS

2.1 TASK ONE. Data Collection and Analysis

2.1.1 Data Collection and Data Preparation

The Contractor shall collect CISA workforce data in accordance with EEOC MD-715 requirements and combine with initial data set furnished by CISA. The Contractor shall also collect additional relevant data for analysis. In so doing, the Contractor shall gather data through individual and group interviews of agency subject matter experts handling the hiring, promotions and leadership training; conduct surveys of targeted populations; access and provide data from available CISA, government-wide, and/or industry sources; combine data into a form suitable for analysis to include preparing, organizing, and ensuring data quality; and follow established or refined protocols for handling information security, storage, and retrieval.

2.1.2 Data Analysis and Interpretation

The Contractor must be able to provide expert services to advise, define, and conduct statistical analyses that provide for high quality (i.e., reliable and valid) conclusions in support of the analysis plan. Such analyses must include, but are not limited to: (a) parametric and nonparametric statistics using simple and multiple linear and non-linear regression analyses; (b) benchmarking and other comparative analyses to available data from other organizations; (c) personnel survey data (e.g. Federal Employee Viewpoint Survey Data and Defense Organizational Climate Survey (DEOCS)).

The Contractor must be able to apply and interpret statistical information to complete standard, EEOC-prescribed analyses, including “glass ceiling,” “blocked pipeline,” “glass wall,” and “low entry-high exit” analyses, as detailed in Barrier Analysis training. The Contractor must include EEOC-created barrier analysis tools (including the EEOC’s “Barrier Analysis: Questions to Guide the Process” guidance) as part of the analysis plan to conduct barrier analysis studies, and may include the EEOC’s root cause analysis tools.Typical barrier analyses use as primary methods, logistic regression, Poisson regression, Chi-Square Analysis, focus groups, interviews, and use as primary datasets, FedHR, Direct Access, or other relevant personnel data, USA Staffing Applicant Flow Data, and FEVS survey data.

The Contractor will provide benchmarks to measure the CISA against including similarly-sized federal agency programs to identify comparative information and best practices related to EEO, assess the applicability of best practices to the CISA, and prepare summary results for presentation to the CISA as needed.

The Contractor shall summarize qualitative data gathered from employee commentary, interviews, focus groups, and other methods. Where appropriate and applicable, qualitative data shall be translated and presented numerically with appropriate assessment of reliability, statistical power, and validity.

The Contractor shall synthesize the summary findings for simple interpretation and as the basis for communication. The Contractor shall provide expert technical advice on the appropriate interpretation of current results, any limits on that interpretation, and an assessment of the power and reliability for the conclusions suggested. The Contractor shall present, to the extent practicable, a neutral and independent review of research findings.

2.2 TASK TWO. Develop Reports and Communications

2.2.1 Barrier Analysis Report

In addition to interim progress reports and real time briefings or interactive presentations of data, the Contractor shall deliver a full and complete consolidated Barrier Analysis report. This report must include but not limited to: (i) Executive Summary; (ii) Introduction; (iii) Literature Review; (iv) Methodology; (v) Data Analysis; (vi) Results; (vii) Discussion; (viii) Conclusion; (ix) Recommendations; and (x) Implementation Plans. The Contractor shall also develop data visualizations and data summaries along with related explanatory text, reports, tools and processes using data visualization tools. The Contractor will provide a presentation of Barrier Analysis Report and findings to OEDIA and designated CISA leadership.

The resulting reports and documents will be subject to review by the CISA. In all cases, the Contractor's timelines and plans must provide for review, revision, and approval by the government of each communication deliverable.

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	6.7	**Post Award Conference**	Within ten (10) business days of task order award or as coordinated by the CO/CS	In person meeting or by virtual meeting
2	6.8	**Draft Contractor Project Plan**	Presented at kick-off meeting	COR, Contracting Officer
3	6.8	**Final Contractor Project Plan**	Within ten (10) business days after kick-off meeting	COR, Contracting Officer
6	6.9	**Progress Reports**	Weekly by COB Wednesday	COR, Contracting Officer
7	2.2.1	**Barrier Analysis Report/Technical Documentation**	8 weeks prior to end of period of performance	COR, APO

5.0 CONTRACTOR PERSONNEL

5.1 Qualified Personnel

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

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.

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

- Project Manager (Oversees all Tasks)

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. 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 0900 and 1700 EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 24 hours of notification. Availability for this contract must be no less than 10 hours per week. The team's routine must be such that the project manager is the go-to source of guidance for contract staff week-to-week, and the primary interface with the agency.

5.4.2 Project Manager Qualifications

- M.S. in a social science (preferred) or other terminal degree in business, public policy, statistics, or a social science (e.g. MBA, MEcon)
- Minimum of five (5) years of experience in social science research projects that require statistical analysis and data analytic reporting
- At least three (3) years conducting workforce analytic projects:
- Minimum of three (3) years of professional experience leading research teams to include:
    - Managing and supervising research teams of at least two (2) team members with varying levels of knowledge or experience (e.g., combining research assistant, subject matter expert, statistician) in an area of social science
    - Developing and executing on a research agenda, with related research designs and analysis plans, in an area of investigation
    - Delivering presentations and leading client meetings
- Demonstrated ability to multi-task and provide analytic support for simultaneous research projects at different stages of completion and to support client contact for more than one project and/or CISA staff member at a time.
- Strong interpersonal skills, including the ability to build strong relationships with clients and analyst staff, effective communication

skills, and flexibility to adapt methods and work practices to CISA's standard procedure and norms
- Minimum of four years of experience with one or more advanced statistical software programs (i.e. STATA, SAS, R) sufficient to independently design, accurately code, and perform statistical analyses

5.5 Non-Key Personnel

5.5.1 Minimum Qualifications

5.5.1.1 Data Scientist

Data Scientist Qualifications:

- Senior to expert level knowledge of professional statistical work such as (a) sampling, (b) collecting, computing, and analyzing statistical data, and (c) applying statistical techniques such as measurement of central tendency, dispersion, skewness, sampling error, simple and multiple correlation, analysis of variance, processing mass statistical data such as tabulating methods or electronic data processing, and tests of significance.
- A degree that included 15 semester hours in statistics (or in mathematics and statistics, provided at least 6 semester hours were in statistics), and 9 additional semester hours in one or more of the following: physical or biological sciences, medicine, education, or engineering; or in the social sciences including demography, history, economics, social welfare, geography, international relations, social or cultural anthropology, health sociology, political science, public administration, psychology, etc. At least Three (3) years of progressive work experience in statistics, as it relates to barrier analysis.

5.5.1.2 Technical Writer

Technical Writer Qualifications:

- A solid understanding of fundamental statistical concepts is essential. This includes techniques for collecting representative data through proper sampling methods. Technical writers should be comfortable collecting, computing, and analyzing data using appropriate software. Furthermore, the ability to interpret statistical results is crucial. This involves analyzing data to measure central tendency (average), dispersion (spread), and skewness (lopsidedness). Technical writers should also be able to assess sampling error and its impact on findings.
- A bachelor's degree in English, communication, or a related field is preferred. This educational background provides a strong foundation in clear and

concise writing, essential for crafting user-friendly technical documentation. While an in-depth statistics background is not required, coursework that includes at least 6 semester hours in mathematics or statistics is recommended. These courses will equip technical writers with the necessary quantitative skills to analyze user feedback data and metrics to improve the clarity and effectiveness of technical documentation.

5.6 Employee Identification

5.6.1 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.

5.6.2 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.

5.7 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.

5.8 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 listed below:

Base: September 30, 2024 to September 29, 2025
Option Year 1: September 30, 2025 to September 29, 2026

Option Year 2: September 30, 2026 to September 29, 2027

6.2 PLACE OF PERFORMANCE

The primary place of performance will be the Contractor's facilities or Contractor's remote location with occasional visits to the Department of Homeland Security facilities in the Washington Metro Area.

6.3 CONTRACTOR TELECOMMUTING – REMOTE PERSONAL RESIDENCE WORK LOCATIONS.

Telecommuting for federal government contractors will be considered on a situational basis to the extent practicable to meet DHS mission needs. Telecommuting allows contractor personnel to perform their contractual requirements outside of CISA office locations, typically at a contractor's personal residence or a corporate telecommuting office location. Telecommuting for contractor personnel provides the government flexibility to meet unique CISA organizational and facility needs and requirements. The goal of telecommuting for contractor personnel is to enhance the delivery of services that support the DHS mission.

Additionally, the provision to permit contractor telecommuting may be revoked at the Task Order level at any time if the Government makes such determination. The telecommuting provision does not change any task order requirements; all other terms and conditions of the task order remain in full force and effect.

6.4 CONTRACTOR LABOR RATES CHARGED WHILE TELECOMMUTING

The contractor shall charge the same applicable fixed hourly rate as for a Government site for those contractor personnel when they telecommute at their designated telecommuting location.

6.5 HOURS OF OPERATION

Contractor employees shall generally perform all work between the hours of 0800 and 1700 EST, Monday through Friday (except Federal holidays). However, there may be occasions when Contractor employees shall be required to work other than normal business hours, including weekends and holidays, to fulfill requirements under this SOW.

6.6 TRAVEL

Contractor travel shall not be required for this requirement.

6.7 POST AWARD CONFERENCE

The Contractor shall attend a Post Award Conference with the Contracting Officer and the COR no later than 5 business days after the date of award. The purpose of the Post Award Conference, which will be chaired by the 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 at the Government's facility, located at 1616 N Fort Myer Dr., Arlington, VA 22209 or via teleconference.

6.8 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 10 business days after the Post Award Conference.

6.10 PROGRESS MEETINGS

The Project Manager shall be available to meet with the COR upon request to present deliverables, discuss progress, exchange information and resolve emergent technical problems and issues. These meetings shall take place via video conference or teleconference.

6.11 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).

6.12 INTELLECTUAL PROPERTY

Any intellectual property developed in response to any task area is the sole property of the CISA, including but not limited to reports, presentations, training materials, and related electronic files, unless a specific written legal agreement is reached on a specific item.

7.0 GOVERNMENT FURNISHED RESOURCES

The Government will provide the following property to the Contractor for work required under this contract:

(1) One Laptop
(2) A Personal Identification Verfication (PIV) Card

The Government will provide the following initial information, data and documents to the Contractor for work required under this contract, within two business days of date of the award:

- MD-715 Reports (Annual EEO Program Status Report)
- Federal Equal Opportunity Recruitment Program Report
- Civil Rights, Diversity & Inclusion Division Annual Reports
- Organizational Assessment Surveys/Reports
- Defense Organizational Climate Survey (DEOCS)
- Civil Rights Strategic Plan
- Diversity and Inclusion Strategic Plan
- Merit Promotion Plan
- Awards and Recognition Program Policy
- Recruitment Plan
- Mentoring Program Policy
- Training Program Policy
- Selection Procedures
- Disciplinary Policy

The Contractor will advise on any additional datasets needed to accomplish the requirements.

The Contractor must use Government furnished information, data and documents only for the performance of work under this contract, and must be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor must not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

8.0 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 2.0 and SOW 7.0.

9.0 INVOICES AND PAYMENT PROVISIONS

In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

1) Cover sheet identifying DHS;
2) 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:

E-mail: [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.

12.0 RECORDS MANAGEMENT OBLIGATIONS

12.1 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.

12.2 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.

12.3 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.

12.4 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.

12.5 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 [contract vehicle]. 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 purchase

order. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

12.6 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.

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

12.8 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.

12.9 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.

12.10 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.

12.11 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.

12.12 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 purchase order, 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.

13.0 SECURITY

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

POST-AWARD INSTRUCTIONS REGARDING SECURITY REQUIREMENTS FOR CONTRACTS/ORDERS

The procedures outlined below shall be followed for the CISA Office of the Chief Security Officer (OCSO), Personnel Security Division (PSD) to process background investigations, Entry on Duty determinations, and Fitness determinations, as required, in a timely and efficient manner.

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

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

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

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

CISA 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 CISA 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 CISA OCSO/PSD.

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

CISA OCSO/PSD shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the COR all CISA-issued identification cards and building passes that have either expired or have been collected from terminated employees. If an identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the pass or card number, name of individual to whom it was issued and the last known location and disposition of the pass or card.

13.1 PROTECTION OF INFORMATION

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

The Government will provide copies of the references cited in SOW 1.4 at the Post Award Conference.

The Contractor shall use Government furnished information, data and documents only for the performance of work under this contract, and shall be responsible for returning all Government furnished information, data and documents to the Government at the end of the performance period. The Contractor shall not release Government furnished information, data and documents to outside parties without the prior and explicit consent of the Contracting Officer.

Contractor access to proprietary 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).

REFERENCES:
DHS Management Directive 140-01, "*Information Technology System Security Program, Sensitive Systems*"

- DHS 4300A Policy Directive (Version 13.3, February 13, 2023).
- DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018 for NSS Collateral (Unclass, Secret or Top Secret Collateral).
- DHS Sensitive Compartmented Information (SCI) Systems 4300C Instruction Manual, Version 2.2, August 22, 2018 for TS SCI/C-LAN

1. SECTION 508 REQUIREMENTS

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.

1.1 508 Requirements for Technology Services (include in the SOW, PWS, or SOO)

1.1.1 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.

1.1.2 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.

1.1.3 When developing or modifying ICT deliverables that contain the ability to automatically generate electronic documents and forms in Microsoft Office and Adobe formats, or when the capability is provided to enable end users to design and author web based electronic content (i.e. surveys, dashboards, charts, data visualizations, etc.), the Contractor shall demonstrate the ability to ensure these outputs conform to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria). The Contractor shall demonstrate conformance by conducting testing and reporting test results based on representative sample outputs. For outputs produced as Microsoft Office and Adobe PDF file formats, the Contractor shall use the test methods published under "Accessibility Tests for Documents", which are published at https://www.dhs.gov/compliance-test-processes. For outputs produced as web based electronic content, the Contractor shall use the DHS Trusted Tester for Web Methodology Version 5.0, or successor versions. This methodology is published at https://www.dhs.gov/trusted-tester

1.2 Section 508 Deliverables (include in the SOW, PWS, or SOO)

1.2.1 **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.

1.2.2 **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.

1.2.3 **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.

2. THE HOMELAND SECURITY PRESIDENTIAL DIRECTIVE 12 (HSPD-12)

- The Homeland Security Presidential Directive 12 (HSPD-12) requires the use of the Personal Identity Verification (PIV) credentials as the common means of authentication for access to DHS facilities, networks, and information systems. Personal Identity Verification (PIV) credentials shall be used as the primary means of logical authentication for DHS sensitive systems. The Contractor must use his or her federal issued Personal Identity Verification (PIV) credentials to access DHS resources to include IT applications and physical facility.

- The DHS Security Office shall be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return to the Contracting Officer Representative (COR) all DHS issued Personal Identity Verification (PIV) credentials/identification cards and building passes that have either expired or have been collected from terminated employees. If a PIV credential/identification card or building pass is not available to be returned, a report shall be submitted to the COR, referencing the PIV credential, pass or card number, name of individual to who it was issued and the last known location and disposition of the PIV credential, pass or card."

3. ARTIFICIAL INTELLIGENCE/MACHINE LEARNING REQUIREMENTS

Definitions: Artificial Intelligence (AI) includes the following: (1) Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets. (2) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning,

communication, or physical action. (3) An artificial system designed to think or act like a human, including cognitive architectures and neural networks. (4) A set of techniques, including machine learning, that is designed to approximate a cognitive task. (5) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

Requirements:
The 2019 National Defense Authorization Act (NDAA) and Executive Order (EO) 13960 require that AI used in the Federal Government foster public trust and confidence while protecting privacy, civil rights, civil liberties, and American values. All federal employees, contractors, and subcontractors, when designing, developing, acquiring, and/or using AI for or within DHS, will adhere to the following 9 principles.

1. Lawful and respectful of our Nation's values: Agencies shall design, develop, acquire, and use AI in a manner that exhibits due respect for our Nation's values and is consistent with the Constitution and all other applicable laws and policies, including those addressing privacy, civil rights, and civil liberties.

2. Purposeful and performance-driven: Agencies shall seek opportunities for designing, developing, acquiring, and using AI, where the benefits of doing so significantly outweigh the risks, and the risks can be assessed and managed.
3. Accurate, reliable, and effective: Agencies shall ensure that their application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective.

4. Safe, secure, and resilient: Agencies shall ensure the safety, security, and resiliency of their AI applications, including resilience when confronted with systematic vulnerabilities, adversarial manipulation, and other malicious exploitation.

5. Understandable: Agencies shall ensure that the operations and outcomes of their AI applications are sufficiently understandable by subject matter experts, users, and others, as appropriate.

6. Responsible and traceable: Agencies shall ensure that human roles and responsibilities are clearly defined, understood, and appropriately assigned for the design, development, acquisition, and use of AI. Agencies shall ensure that AI is used in a manner consistent with these Principles and the purposes for which each use of AI is intended. The design, development, acquisition, and use of AI, as well as relevant inputs and outputs of particular AI applications, should be well documented and traceable, as appropriate and to the extent practicable.

7. Regularly monitored: Agencies shall ensure that their AI applications are regularly tested against these Principles. Mechanisms should be maintained to supersede, disengage, or deactivate existing applications of AI that demonstrate performance or outcomes that are inconsistent with their intended use or this order.

8. Transparent: Agencies shall be transparent in disclosing relevant information regarding their use of AI to appropriate stakeholders, including the Congress and the public, to the extent practicable and in accordance with applicable laws and policies,

including with respect to the protection of privacy and of sensitive law enforcement, national security, and other protected information.

9. Accountable: Agencies shall be accountable for implementing and enforcing appropriate safeguards for the proper use and functioning of their applications of AI, and shall monitor, audit, and document compliance with those safeguards. Agencies shall provide appropriate training to all agency personnel responsible for the design, development, acquisition, and use of AI.