DEPARTMENT OF HOMELAND SECURITY (DHS)

STATEMENT OF WORK (SOW)
FOR
CONNECTED COMMUNITIES RISK MANAGEMENT INITIATIVE

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 Management and Business Service Offices and six Divisions: The Cybersecurity Division (CSD), the Emergency Communications Division (ECD), the Infrastructure Security Division (ISD), the Stakeholder Engagement Division, the Integrated Operations Division (IOD), as well as, the National Risk Management Center (NRMC), which are headquartered with the National Capital Region (NCR).

1.2 SCOPE

The contractor will assist the NRMC by providing the classified Top Secret technical functions necessary to support the Center's business processes and mission-related risk management initiative related to connected communities. Successfully supporting these functions will require contractor expertise in strategic consulting, identification of technology risks related to connected communities, risk data and technical analysis and assessments, identification of risk-trends that lead to development of risk mitigation strategies. Whole-of-NRMC collaboration is critical for success of the activities.

1.3 OBJECTIVES

CISA recognizes that the cyber-attack surface increases as systems and services become more interconnected and interdependent due to the increased number of users, applications, and data access points enabling the potential for malicious activity and cybersecurity compromise. The potential impacts of these risks have generated significant interest from both the Department of Homeland Security (DHS) and CISA leadership and falls well within the NRMC's role of analyzing, prioritizing, and managing the most significant risks to national critical infrastructure. The NRMC will partner with other CISA divisions, interagency partners, industry representatives, and State, Local, Tribal, and Territorial (SLTT) stakeholders to develop, organize, and coordinate risk mitigation strategies relating to smart and connected technologies as part of the CISA Connected Communities Initiative (CCI).

The desired objectives are to:

- Support government personnel as they manage risks related to technologies within Connected Communities by providing risk identification, understanding risk analysis functions, and development of risk mitigation functions at the Top Secret/SCI

classification level.
- Support government personnel in ensuring collaboration of activities (including assessment activities) across NRMC

Deliverables and Initiative support will be used by the government to: 1) understand technologies and the associated risks, 2) identify and analyze risks, and 3) share risk information with stakeholders in order to reduce risk to federal networks and the networks of America's critical infrastructure.

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:

a) DHS Sensitive Systems Policy Directive 4300A, Version 13.1, July 27, 2017
b) DHS National Security Systems Policy Directive 4300B, Version 10.1, November 21, 2018
c) DHS Sensitive Compartment Information (SCI) Systems 4300C Instruction Manual, Version 2.2, August 22, 2018
d) Modeling Capability Transition Environment (MCTE) Technical Specifications Guide, (DRAFT), December 9, 2019

These documents can be provided upon request.

1.4.2 Reference Documents

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

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 2.1, March 24, 2017 for TS SCI/C-LAN.

2.0 SPECIFIC REQUIREMENTS/TASKS

Contractor will require access to classified information at the Top-Secret level under this SOW. The maximum level of classification is Top Secret/Sensitive Compartmented Information (TS/SCI). Access to classified information will be specified in a Department of Defense Contract Security Classification Specification (DD Form 254) issued with the resultant order (s), if

applicable. FAR 52.204-2 Security Requirements is applicable to this Task Order.

Vendors must have a DCSA issued Top Secret facility clearance at quote submission and maintained through the life of the Task Order.

The following Contractor personnel: Operations Specialist, Industrial Engineer, and Operations Research Analyst are required to possess, and retain a Top Secret (TS) Clearance, and be eligible to obtain and retain Sensitive Compartmented Information (SCI) eligibility/access provided by DHS, throughout the life of the Task Order. All other contractor personnel will require access to Unclassified FOUO information.

2.1 TASK ONE. Connected Communities Risk Management

The Contractor shall provide support for risk management activities, which include: identifying and understanding the technologies within connected communities and their risks; analyzing risk information; developing risk mitigation strategies; sharing risk information with various stakeholders; and assessing the success of any risk mitigation activities implemented by the stakeholder. This Task is broken down into sub-tasks as follows:

2.1.1 Identify technologies and risks

The Contractor shall conduct research on smart, connected, and emerging technologies to identify new risk considerations and requirements relevant to the Initiative as well as risk trends in implementation of these technologies.

2.2.1.1 Identify key partners, stakeholders, and communities of interests to provide knowledge and understanding of who is doing what in the smart, connected, and emerging technologies focus areas.
2.2.1.2 Engage with partners and stakeholders to identify ongoing research and development activities across the communities of interest to fully understand risk issues, concerns, and gaps that CISA may be able to address.
2.2.1.3 Identify both current and future risk considerations.
2.2.1.4 Engage with partners and stakeholders to identify current and future trends.
2.2.1.5 Plan and conduct workshops or listening sessions to do trends analysis activities

2.2.2 Technical data analysis and assessments

The Contractor shall lead risk and technical data analysis and assessments on smart, connected, and emerging technologies as required by the government. Also, the Contractor shall establish the methodology and operationalize the technical analysis requirements gathering and validation process for potential Connected Communities projects and activities.

2.2.2.1 Develop a Risk Analysis and Assessment Plan that identifies risk gaps and considerations and formulate activities to coordinate and execute the Plan with partners and stakeholders. Analysis may include written reports assessing risks to critical infrastructure and citizen privacy related to the use of technologies such as IoT, AI, cloud computing, quantum computing, and operational technology.

2.2.2.2 Coordinate, lead, and support Working Groups or partnership collaboration to manage Plan development and implementation activities.

2.2.2.3 Manage metrics, reporting, and key performance indicators related to risk mitigation effectiveness

2.2.3 Develop information-sharing products

The Contractor shall develop research materials, technical papers, briefing materials, and recommendations for decision makers.

2.2.3.1 Develop and coordinate peer-reviewed research materials and technical papers

2.2.3.2 Respond to Request for Information and Request for Action (RFI / RFA) as required.

2.2.4 Establish methodology and operationalize technical analysis

The contractor shall establish the methodology and operationalize the technical analysis requirements gathering and validation process for potential CCI projects and activities.

2.2.4.1 Develop and manage the Risk Analysis and Assessment Plan.

2.2.4.2 Coordinate, lead, and support Plan development and implementation activities.

2.2.5 Identify trends supporting risk mitigation strategies

The contractor shall identify trends in the implementation of smart, connected, and emerging technologies to support development of risk mitigation strategies

2.2.5.1.1.1 Engage with partners and stakeholders to identify current and future trends.

2.2.5.1.1.2 Plan and conduct workshops or listening sessions to do trends analysis activities

2.3 TASK TWO. Additional (Surge) Support - Optional

The Contractor shall support the NRMC's missions and priorities, which are subject to change as a result of priorities realigned by the senior leadership of DHS, the Congress, or the President. The Government may require optional in-scope surge support to perform increased support of the defined Task 1 requirements in this SOW, included above in sections 2.2.1 through 2.2.5.

Surge Support is an optional Contract Line Item (CLIN), which may be executed by the Contracting Officer in accordance with FAR 52.217-7 Option for Increased Quantity – Separately Priced Line Item, and in compliance with FAR 17.207. The Contracting Officer may exercise the option by written notice to the Contractor within 15 days of execution.

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 10 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	6.9	**Post Award Conference**	10 days after award	N/A
2	6.8	**Final Contractor Project Plan**	15 days after award	COR, Contracting Officer
3	6.4	**Telecommuting Plan (unclassified work)**	30 days after award	COR, Contracting Officer
4	6.11	**Progress Reports**	10th day of the month	COR, Contracting Officer
5	7.1	**Master Inventory Report**	Monthly	COR, APO
6	7.0	**Receipts for Purchased CISA Property**	Within 5 Business days of purchase	COR, APO
7	7.3	**Monthly Asset Management Report**	Monthly	COR, APO

8	7.0	**Invoices/packing slips/receipts for property purchased for CISA**	Monthly with the Asset Management Report	COR, APO
9	2.2.2.1	**Risk Analysis and Assessment Plan**	As required	COR, Contracting Officer
10	2.2.3	Information-Sharing Products	As required	COR, Contracting Officer

5.0 CONTRACTOR PERSONNEL

5.1 Qualified Personnel

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

Senior: Industrial Engineer
An industrial engineer shall design, develop, test, and evaluate integrated systems for managing industrial production processes, including human work factors, quality control, inventory control, logistics and material flow, cost analysis, and production coordination. Excludes "Health and Safety Engineers, Except Mining Safety Engineers and Inspectors" (17-2111). A bachelor's degree (BA/BS) with industrial engineering degree (or equivalent) or civil engineering degree (or equivalent) with a minimum of 7 years work experience 4 years of experience with a Masters (MA/MS) in Industrial Engineering degree (or equivalent) or Civil Engineering degree (or equivalent).

Senior: Operations Research Analyst

An Operations Special Analyst shall: conduct research on smart, connected, and emerging technologies to identify new risk considerations and requirements; lead risk and technical data analysis on smart, connected, and emerging technologies; develop recommendations; operationalize the technical analysis requirements gathering and validation process for potential connected communities activities; and identify trends in the implementation of smart, connected, and emerging technologies to support development of risk mitigation strategies. They will also formulate and apply mathematical modeling and other optimizing methods to develop and interpret information that assists management with decision making, policy formulation, or other managerial functions. May collect and analyze data and develop decision support software, service, or products. May develop and supply optimal time, cost, or logistics networks for program evaluation, review, or implementation. A bachelor's degree (BA/BS) in operations research degree (or equivalent) with a minimum of 7 years work experience or 4 years of experience with a Masters (MA/MS) in Operations Research degree (or equivalent).

5.2 Key Personnel

One of the of the labor categories will be the Key Personnel Team Lead for this requirement.

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.

5.2.1 Team Lead/Operations Specialist: Subject Matter Expert

A Subject Matter Expert in Urban and Regional Planning shall develop comprehensive plans and programs for use of land and physical facilities of jurisdictions, such as towns, cities, counties, and metropolitan areas. A bachelor's degree (BA/BS) in Urban and Regional Planning degree (or equivalent) with a minimum of 7 years work experience or 4 years of experience with a Masters (MA/MS) in Urban and Regional Planning degree (or equivalent).

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

The Team Lead shall have experience managing projects relating to private and public sector information sharing. The Team Lead shall have developed and implemented process methodologies and Agency or Corporate-level Strategic Plans for transition development projects. The Team Lead shall have experience leading teams working in a fast-paced environment with private sector stakeholders (e.g., other than federal consulting).

The Team Lead shall be available to the COR via telephone between the hours of 8:30 am and 5:00 pm EST, Monday through Friday, and shall respond to a request for discussion or resolution of technical problems within 48 hours of notification.

5.3 Continuity of Support

The Contractor shall ensure that the contractually required level of support for this requirement is always maintained. 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.

5.4 Employee Identification

5.4.1 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.

5.4.2 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.

5.5 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 SECURITY

Contractor access to classified information is required under this SOW. The maximum level of classification is Top Secret/SCI. The details will be specified in a draft Department of Defense (DD) Form 254.

Contractor must possess and retain an active final Top-Secret security clearance granted by the Defense Counterintelligence and Security Agency (DCSA) at the time of solicitation/proposal submission.

The following positions will require TS-SCI: Operations Specialist, Industrial Engineer, and Operations Research Analyst. Contractor will require access to classified information at the Top-

Secret level under this SOW with access to Sensitive Compartmental Information (SCI) during the performance of duties granted by DHS.

- Required to possess and retain a Top Secret (TS) Clearance.
- Required to be eligible to be granted and retain Sensitive Compartmented Information (SCI) eligibility/access by DHS.

All other contractor personnel will require access to Unclassified FOUO information.

Safeguarding of classified information at the contractor facility is not authorized. All access to classified information will be at the government location as specified in the place of performance. Access to classified information will be accessed solely from CISA facilities. The details will be specified in the Department of Defense Contract Security Classification Specification (DD Form 254).

Contractor access to CISA Sensitive Information, systems, networks and reoccurring access to CISA facilities is required under this SOW; therefore, contractor employees will require DHS Fitness Determination to perform work. Sensitive Information is defined in the DHS Instruction Handbook, 121-01-007, "The Department of Homeland Security, Personnel Security, Suitability and Fitness Program" as "Any information, the loss, misuse, disclosure, unauthorized access to, or modification of, which could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria by an Executive Order or an Act of Congress to be kept secret in the interests of national defense, homeland security, or foreign policy (End of Definition). This definition includes one of the following categories of information:

A. Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. section 21 1-224; its implementing regulations, 6 C.F.R. Part 29; or the applicable PCII Procedures Manual; or
B. Sensitive Security Information (SSI), as described in 49 C.F.R. Part 1520; or
C. Sensitive but Unclassified Information (SBU) -For Official Use Only -, which consists of any other information which:

(1) When information is provided by the government to the contractor, information will be marked with the appropriate dissemination markings (FOUO/SBU, etc.).

(2) Is designated "sensitive" in accordance with subsequently adopted homeland security information handling requirements."