DEPARTMENT OF HOMELAND SECURITY (DHS)

Statement of Work

FOR

Holistic Soft Target Risk Assessment Engine and Recovery Resources Conducted by National Center of Excellence for National Counterterrorism, Innovation, Technology, and Education (NCITE) Center, University of Nebraska at Omaha (UNO)

I. Purpose

The Department of Homeland Security Science & Technology Directorate (DHS S&T) seeks a response from the National Counterterrorism Innovation, Technology, and Education Center (NCITE), a DHS Center of Excellence led by the University of Nebraska Omaha, to perform research/scientific services that are within scope under the Basic Ordering Agreement (BOA) # 70RSAT21G00000002.

II. Background and Project Objective

The University of Nebraska at Omaha leads the U.S. Department of Homeland Security's (DHS) National Counterterrorism Innovation, Technology, and Education (NCITE) Center. This Center was established from the DHS Terrorism Prevention and Counterterrorism Research Center of Excellence grant competition in 2020. NCITE is thus a federally funded academic consortium based in Omaha that brings in 50+ academics from 29 partner institution to conduct a range of activities including basic and applied research, and education and training initiatives to support and enhance DHS analytic efforts.

Soft targets (e.g., schools, churches, stadiums, malls) are vulnerable to increasing cyber, natural, and physical threats. Soft targets vary in size and available resources to invest in security. This critical infrastructure asset class is comprised of many small organizations that lack security resources and training. These small organizations typically do not have trained and dedicated security staff, experienced security assessors, and struggle with courses of action to take to increase their security posture and protect against man made and natural threats. More directly, there are so many assets that it is not feasible for DHS to visit or support each facility. For example, there are over 125,000 public and private schools in the US and approximately 350,000 church buildings. As such, we offer that a necessary path forward to support soft targets is providing risk assessment tools and information to assist them in managing their risks. A risk assessment is a product or process which collects information and assigns value to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decision making (from DHS Risk Lexicon). This risk assessment approach increases resiliency through looking at the holistic lens of risk – protection, mitigation, response, and recovery against all threats – physical, cyber, dependencies/interdependencies, and supply chain.

With these end-users in mind, one goal of this project is to provide deployable risk assessment tools that can be used by small, or resource constrained soft targets. The core of the tool is the development of a risk

engine in Tasks 1-3 focused on K-12. The risk engine will incorporate all elements of risk—threat, vulnerability and consequence. It will leverage subject matter expert guidance on best actions to take with emphasis on no-cost and low-cost solutions. The risk engine will address a high need in the soft target community, leverages existing research and expand on emerging methods in measurement and assessment. The need for such a risk engine was identified via a combination of internal subject matter expertise, review of existing CISA projects, and communication with stakeholders at SED and ISD at CISA. This iterative process will allow for the development of a risk engine based on a systematic process utilized in the risk management community. It will also leverage work in CISA – 15-year vulnerability assessment tool created by the Enhanced Critical Infrastructure Protection Program (ECIP). The ECIP is currently deployed nationally and is a key tool for the assessment of critical infrastructure. The methodology will also leverage the CISA Security Planning Workbook. Both the workbook and ECIP will provide the foundation for the methodology.

This project will cover the spectrum of threat identification, prevention, and response with a focus on the provision of recovery resource. As articulated in the FY24 Proposal List, the work undertaken in Task 4, a second goal of the project will be to facilitate the requirements associated with ISD's *All-Hazard Recovery Resources to Support K-12 Schools and School Systems* by assisting schools in the identification of vulnerabilities to allow for the more efficient application of available resources to recover from an event and increase resiliency to facilitate prevention, protection, and mitigation in the future.

The proposed soft-target assessment tool will be built using next generation human interface elements and leverage chat interaction. The proposed system will be designed to meet contemporary preferences for engaging, intuitive, and user-friendly interfaces. This alignment improves usability, accessibility, and user satisfaction, while also contributing to the precision of data entry and enhancing the user's grasp of system prompts and the information provided. The result of using these emerging technologies should be an assessment tool that is easier to complete, more satisfying to use, and more likely to be completed, resulting in generated output that has increases the likelihood of behavioral change on the part of the user. Soft targets will be better protected when better data are generated.

A simplistic, actionable, all-hazards risk assessment tool is needed to help this critical soft target infrastructure subsector to me more secure and resilient. The tool will pilot K-12 after deployment and then expand to other soft target categories (e.g., churches/synagogues, stadiums, malls) based on resources and demand signal from CISA and other stakeholders. More directly, the tool will be built in such a way as to allow for adaptability in application to other soft target variants. Increasing access to recovery resources for common threats will also increase community responsive and long-term resilience if a negative event were to occur.

III. Statement of Work:

This SOW includes four (4) task areas:

- Task 1) Task and Task Administration Support,
- Task 2) Risk Assessment Literature Review

- Task 3) Risk Engine (Scoring) Development & Common Threat Identification
- Task 4) Identify Gaps and Develop Recovery Resources Based on Common K-12 Threats

Task 1: Task and Task Administration Support (for all subsequent tasks)

Key Deliverables:

1. ***Project Plan***
   The Contractor shall deliver a project plan for all tasks. The Project Plan shall include, at a minimum:
   - Project schedule
   - Spend plan
   - Identification of key personnel
   - Key milestones and deliverables
   - Risk assessment
   - Compliance documentation as needed
   - Data collection plan

2. ***Deliverable Reviews***
   The Contractor shall conduct deliverable reviews with the Government for all tasks. Deliverable reviews shall take place no later than 10 days after completion of each deliverable. Deliverable reviews will vary in formality depending on the nature of the engagement. The Contractor shall recommend a level of content and formality of each review within the Project Plan which may range from a teleconference to an in-person discussion supplemented with a written presentation and documentation.

3. ***Monthly Status Reports***
   The Contractor shall provide monthly status reports for all tasks to the Government in a template provided by the Program Manager for the duration of the period of performance. The report shall include:
   - Technical progress
   - Schedule performance (actual vs. planned)
   - Cost performance (actual vs. planned)
   - Technical level risks and issues

   Each monthly status report shall update the projected delivery dates of future deliverables. Each projected delivery date that has changed from the previous month, an explanation shall be provided of the cause of the change. The monthly status report shall also track action items assigned to all parties, including the Government, and identify events in the next 30 working days (i.e., key meetings). The contractor shall have monthly meetings with DHS reviewing the monthly progress reports, technical discussions, and deliverables. There may be technical discussions some months that require in-person meetings either in Washington, DC or Omaha, NE.

4. ***Task Kick-Off Meeting***
   An initial kick-off meeting will be held within 15 calendar days of award or as agreed to by the Task Order Contracting Officer Representative (COR) and will be attended by the Task Order Program Manager, COR, and the Task Order Contract Specialist/Contracting Officer. Key Contractor personnel as well as a representative from the Contractor's contracts organization are required to participate. Kick-off meetings may be conducted in person or by conference/video call. The intent of the kick-off is for all key personnel to meet to discuss the projects overall technical and contractual requirements. At this meeting, the Contractor shall be prepared to discuss the following:
   - Technical Objectives
   - Preliminary Project Plan refine and assess the Project Plan
   - Roles and responsibilities of key contractor and Government personnel
   - Deliverables and Deliverable Acceptance Criteria
   - Performance Review
   - Reporting and Invoice Requirements
   - Potential Risks (e.g., Institutional Review Board, Protected Critical Infrastructure Protection data)

5. ***Task Close-Out Meeting***
   The Government and the Contractor shall hold a Task Close-Out meeting for all subsequent tasks. The contractor shall assemble final project deliverables and present a detailed overview of findings to the DHS S&T Program Manager, up to 30 days before the end of the period of performance.

Task 2: Risk Assessment Literature Review

The purpose of this task is to collect relevant information on the current state-of-the-art in regard to risk assessment methodologies, data, and tools (within DHS as well as external sources) to identify potential capabilities to leverage and finalize the implementation plan for data collection, development of the risk engine, and IT architecture design.

Key Deliverables:

6. **Literature Review**
   Market survey of risk assessment tools and methodologies. The contractor shall conduct a rigorous review of relevant threat, vulnerability, and risk assessment methodologies, checklists. Literature review will be broad across all critical infrastructure sectors with emphasis on applicability to soft targets and especially K-12 subsector. Focus should be on all hazards including physical security, cybersecurity, and natural disasters. Review should also include screening tools, quantitative risk engines, and cross-sector/dependencies considerations along with the initial information provided by DHS. At a minimum, include the following in the review:

   Methodologies/Reports
   - DHS Risk Lexicon,

- DoE Readiness and Emergency Management for Schools (REMS) Technical Assistance Center (e.g., cybersecurity, best practices, school safety strategies, state agency roles, resilience strategies, earthquake preparedness, crime prevention, family reunification, emergency management, lockdown/shelter-in-place guidance, chemical management planning for toxic materials, school behavioral threat assessments, communications and warning considerations, developing emergency operations plans, evacuation guidance, tabletop exercises),
- 2023 National Summit on K-12 School Safety and Security Resource Guide,
- USSS A Toolkit for Strengthening K-12 Reporting Programs,
- CISA Security Planning Workbook,
- CISA K-12 Cybersecurity Report and Toolkit,
- Sector Risk Assessment List,
- Enhanced Critical Infrastructure Protection methodology and analysis,
- Chemical Facility Anti-Terrorism Standards (CFATS),
- Security Assessment at First Entry (SAFE),
- CISA Physical Performance Goals (e.g., Physical Security Performance Goals for Faith-Based Communities),
- CISA Houses of Worship Security Self-Assessment and User Guide,
- CISA Protecting Places of Worship: Six Steps to Enhance Security Against Targeted Violence,
- CISA Common Vulnerabilities, Threats, and Protective Measure Report Series,
- Homeland Security Materials (e.g., Connect, Plan, Train, Report),
- SchoolSafety.gov cybersecurity, phishing, protecting kids, and
- CISA Cybersecurity Performance Goals.

Tools

- REMS SITE ASSESS,
- REMS EOP ASSESS,
- REMS Toolbox (e.g., state and local school tool repository),
- CISA School Security Assessment Tool (SSAT),
- CISA Technical Resource for Incident Protection (TRIPwire),
- CISA K-12 Cybersecurity Report and Toolkit,
- CISA Gateway,
- CISA Infrastructure Survey Tool (IST),
- CISA Cyber Infrastructure Survey Tool (Cyber IST), and
- Rapid Response Infrastructure Survey Tool (Rapid IST).

DHS will provide other relevant background materials and the contractor will supplement the background materials through open-source literature reviews, stakeholder and subject matter interviews, and conducting expert panel sessions. There are two deliverables for this task.

1) Develop a technical document and/or spreadsheet summarizing sources analyzed and initial recommendations on what can potentially be leveraged, and where gaps address.
2) Provide a presentation to DHS summarizing the technical document and/or spreadsheet.

Task 3: K-12 Risk Engine (Scoring) Development & Common Threat Identification

The purpose of this task is to develop the risk engine that includes the question set, quantitative scoring process, and the analysis and reporting for the K-12 subsector; however, the risk engine should be designed to be adaptable to other soft target categories.

Key Deliverables:

7. **Collective Analysis**
   Concurrently, leveraging literature review (Task 2), vet information with various stakeholders and subject matter experts to potentially expand landscape of existing risk capabilities that includes cyber and physical security, supply chain, infrastructure dependencies/interdependencies, and all hazards (e.g., natural disasters, insider threat). Organize expert panel discussions (as needed) to develop comprehensive repository of risk assessment materials prioritize literature review findings and identify gaps and stakeholder requirements. Identify common threats and additional related risk assessment data, tools and methodologies that can be leveraged to refine the initial set of baseline items, prioritize threats and vulnerabilities, pinpoint potential consequences and associated risks, prioritize risks, and identify protective measures tailored to each soft target category, considering available resources such as those provided by DHS and other options. The contractor shall deliver a presentation to DHS summarizing the task results along with providing a technical report.

8. **Common Threat Identification**
   Based on the collective analysis, the contractor shall deliver a presentation to DHS identifying common threats which will be the basis for Task 4.

9. **Question Set Finalization**
   Leveraging previous tasks (Task 2 and Deliverable 7 - Collective Analysis), develop final question set following decision support and risk principles to allow for consistent answering and quantitative scoring. The final question set needs to consider brevity of stakeholder time versus comprehensiveness to calculate risk. Identify questions across soft target categories as well as K-12 specific questions. The contractor shall deliver a written report of the final question set. The contractor shall deliver draft, interim, and final question sets along with providing a presentation to DHS on the final question set.

10. **Risk Engine Development**
    Develop a risk engine from the final question set that takes into consideration threats, vulnerabilities, consequences, and risks to soft targets for K-12. Formulate expert panels to strategize and develop weights to quantitatively measure risk from threats, vulnerabilities and consequences. The contractor shall provide a technical presentation on risk engine approach to be taken. This includes discussing risk methodology solution, defensibility, and adaptability to other soft target areas. It is likely that the technical presentation will be required as an in-person meeting. Contractor shall produce technical report that documents the risk engine methodology.

11. **Risk Engine Prototype**
    Prototype risk engine in a spreadsheet or database system. Spreadsheet or database should have all weights and aggregation included. This should also include examples of reporting analysis that is vetted and refined with stakeholders. Output from the risk engine needs to risk based and sound, and actionable for users of the tool. Iterate with stakeholders as needed to get feedback. The contractor shall provide a presentation of findings as well as provide the spreadsheet or database of the risk engine prototype along with any documentation needed to use the spreadsheet or database.

12. **Risk Engine Pilot**
    Conduct at least 3 pilot projects working through the question set, methodology, risk engine (and reporting) with different K-12 organizations. Utilize the pilot to refine the question set, methodology, and risk engine as needed. Conduct usability testing to identify any issues and gather user feedback to improve the product design and functionality. The pilot will also help verify functionality, performance, and usability. The contractor shall provide summary brief on pilot and modifications to question set, methodology, and risk engine as needed.

Task 4: Identify Gaps and Develop Recovery Resources

There is a critical need to understand what capacity-building (and scalable) recovery resources are needed to support K-12 schools and organizations against the many hazards, risks, and threat they experience. The purpose of this task is to assess current recovery needs across the identified threat landscape and to identify available resources for K-12 organizations; identify and prioritize capability gaps; and/or develop doctrine, methodologies, and tools to address gaps.

Key Deliverables:

13. **Preliminary Report**
    This will include a preliminary synthesis and review of materials on the K-12 threat landscape. In addition, this deliverable will provide an initial overview of recovery resources and practices for K-12 schools. Documentation of any known federal resource gaps identified at this point in the project will be included.

14. **Threat Landscape (Data and Report)**
    This includes a report of K-12 schools, including (but not limited to): threats of terrorism and targeted violence; civil unrest, matters concerning public health; cyberattacks; bombing-related incidents; mental health challenges among student and staff populations; mis-, dis-, and malinformation campaigns; natural hazards; and other criminal activity or events that may impact school operations. The Threat Landscape Report will include interviews with a small cadre of school safety subject matter experts (SMEs). Interviewees will be identified in collaboration with DHS. Report will leverage information collected as part of Task 3 to validate a set of common threats from which to develop existing resources.

15. **Existing Resources Available (Report/List)**

This includes identification of resources currently available to counter common threats for examination, to include: recovery information sharing among similar audiences or organizations; mental health resources for students and staff; impacts of repetitive drills and exercises on affiliated K-12 audiences (to include parents and the community at large); reunification planning development and implementation; continuity of operations planning and implementation; and additional recovery practices for K-12 campus and community physical infrastructure.

16. **Resource Gap Analysis (Process and Report)**
This includes documentation and prioritization of gaps among current federal resources to determine which (if any) doctrines, methodologies, and/or tools should be the focus of additional research and development. Deliverable will be applied to Toolkit development task outputs, product development, and future research and development funding requests.

17. **Toolkit Development**
This includes the development of initial capacity-building resources for common threats to address identified gaps and roadmaps for future efforts. CISA's School Safety Task Force will transition deliverables via current practices relevant to K-12 stakeholders and audiences. Additionally, efforts will align with requirements as part of the Federal Clearinghouse on School Safety Evidence-Based Practices and CISA Director's Priority engagement directives.
    - Depending on output from previous task, develop checklists, spreadsheets, guidance documents, etc. to begin to mitigate the gaps identified and to provide resources that will assist K-12 in the recovery phase of risk.

IV. Technical Deliverables

Task 1: Task and Task Administration Support (for all subsequent tasks)			
Deliverable	**Completion Date**	**Deliverable Description**	**POC / Recipient**
1	Award + 2 Months	Project Plan for all tasks	DHS COR, DHS PM
2	Delivery + 10 Days	Deliverable Reviews for the Project Plan	DHS COR, DHS PM
3	Monthly for Life of Award	Monthly Status Report(s) for all subsequent tasks	DHS COR, DHS PM
4	Award + 15 Days	Task Kick-Off Meeting	DHS COR, DHS CO, DHS PM
5	Final Deliverable + 10 Days	Task Close-Out Meeting all subsequent tasks	DHS COR, DHS CO, DHS PM
Task 2: Risk Assessment Literature Review			
Deliverable	**Completion Date**	**Deliverable Description**	**POC / Recipient**
6	Award + 6 Months	Literature Review Findings	DHS PM
Task 3: K-12 Risk Engine (Scoring) Development & Common Threat Identification			
Deliverable	**Completion Date**	**Deliverable Description**	**POC / Recipient**
7	Award + 9 Months	Collective Analysis Finding	DHS PM
8	Award + 11 Months	Common Threat Identification	DHS PM
9	Award + 16 Months	Final Question Set	DHS PM
10	Award + 18 Months	Risk Engine Development	DHS PM
11	Award + 23 Months	Risk Engine Prototype	DHS PM
12	Award + 23 Months	Risk Engine Pilot	DHS PM
Task 4: Identify Gaps and Develop Recovery Resources Based on Common K-12 Threats			

Deliverable	Completion Date	Deliverable Description	POC / Recipient
13	Award + 8 Months	Preliminary Report	DHS PM
14	Award + 14 Months	Threat Landscape (Data and Report)	DHS PM
15	Award + 16 Months	Existing Resources Available (Report/List)	DHS PM
16	Award + 18 Months	Resource Gap Analysis (Process and Report)	DHS PM
17	Award + 23 Months	Tool Kit Development	DHS PM

V. Other Contract Details

A. Period of Performance.
Twenty-four (24) months from date of award.

B. Travel.
Travel may be required in the performance of duties listed herein. The DHS S&T COR must approve all travel. All travel and other direct costs associated with the execution of the tasks indicated in this SOW will be reimbursed in accordance with the limits set forth in the Federal Travel Regulations, provided the performer provides appropriate supporting documentation.

C. DHS-Furnished Information.
DHS will provide certain DHS information, materials, and forms unique to DHS to UNO-NCITE to support certain tasks under this SOW.

The DHS S&T COR identified in this SOW will be the point of contact (POC) for identification of any required information to be supplied by DHS.

UNO-NCITE will prepare any documentation according to the guidelines provided by DHS.

D. DHS-Furnished Facilities, Supplies, and Services.
If work at DHS-provided facilities is necessary for the services being performed under this SOW, such facilities will be provided at S&T's office in Washington, DC. Parking facilities are not provided; however, several commercial parking facilities are located near S&T's office. Basic facilities such as workspace and associated operating requirements (e.g., phones, desks, utilities, desktop computers, and consumable, general purpose office supplies) will be provided to NCITE/UNO personnel working in S&T's office.

E. Place of Performance.
The UNO-NCITE will perform the work under this SOW primarily at the selected Center's location. The NCITE partners/subcontractors will perform their work primarily at their own locations.

F. Government Furnished and Contractor Acquired Property.
a. UNO-NCITE shall be accountable to DHS for personal property (1) provided by DHS as Government Furnished Equipment (GFE); or (2) that is Contractor Acquired Property (CAP) acquired with DHS funds where (a) the CAP has an acquisition cost of $5000 or more or (b) where the CAP is sensitive assets of any value, defined as laptops, cameras, Ironkeys, and any other property that may have retainable storage memory.

b. UNO-NCITE shall provide a listing of all GFE or CAP to the DHS Contracting Officer annually on the anniversary date of this task order.

c. Ninety (90) days prior to the completion of work and acceptance of all deliverables under this task order, UNO-NCITE shall provide the DHS Contracting Officer the final and complete listing of all GFE and CAP charged to this task order with an acquisition cost of $5,000 or more or sensitive assets.

d. The DHS Contracting Officer will provide UNO-NCITE with instructions for disposition of all GFP and CAP and provide any additional funds to enable that disposition, as necessary.

G. Deliverables.
UNO-NCITE will provide all deliverables (interim and final technical reports) identified in this SOW directly to the DHS S&T COR and DHS Contracting Officer.

H. Program Status Reports.
UNO-NCITE will deliver monthly status reports to the DHS S&T COR, CO, and DHS S&T Financial Analyst the 15th day of each month containing metrics pertaining to financial, schedule, and scope information, risk information, and performance assessment information of all work performed hereunder. This document will describe the previous 90 calendar days' activity, technical progress achieved against goals, difficulties encountered, recovery plans (if needed), plans for the next 30 calendar day period, and financial status.

I. Invoices.
UNO-NCITE will deliver a monthly invoice to InvoiceSAT.Consolidation@hq.dhs.gov on the 15th day of each month.

J. Information Release.
Prior to releasing any information developed using funds awarded under this contract (or task order, as applicable), UNO-NCITE must route all materials to the S&T COR who will ensure DHS S&T has approved the content release. Please allow a minimum of three weeks for the review and screening of such information (including but not limited to articles, presentations, videos, speeches at conferences, pamphlets, and other forms of printed media) to ensure that such information's release does not violate security policies and procedures.

K. Security Requirements.
All work performed under this SOW is unclassified unless otherwise specified by DHS. UNO-NCITE will not have access to any sensitive information under this task order.

DHS may exercise full control over granting, denying, withholding, or terminating unescorted access to DHS facilities, DHS systems, and/or sensitive DHS information for government/contract employees. Access will be based upon the results of a DHS fitness/suitability investigation. DHS may, as appropriate, make favorable entry of duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the government/contract employee to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full DHS fitness/suitability authorization will follow. The granting of a favorable EOD decision or a full DHS fitness/suitability authorization determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the contract/task order. No employee of the government/contractor shall be allowed unescorted access to a DHS facility, access to any sensitive DHS information, or access to DHS Systems without a favorable EOD decision or DHS fitness/suitability determination by the DHS HQ Office of Security. Government/contract employees assigned to the contract/task order not needing access to sensitive DHS

information, DHS systems, or access to DHS facilities will not be subject to DHS fitness/suitability screening. Government/contract employees waiting on an EOD decision may not begin work on the task order. Limited access to DHS facilities is allowable prior to the EOD decision if the government/contract employee is escorted by an approved DHS employee. This limited access is to allow government/contract employees to attend briefings, nonrecurring meetings, and begin transition work. During one's limited access the government/contract employee will not have access to sensitive or classified DHS information.

The Contractor will have access to the following types of controlled unclassified information (CUI):

- Protected Critical Infrastructure Information, for the purpose of completing Tasks 1-3 of the SOW.
- Personally Identifiable Information (PII), for the purpose of completing Tasks 1-3 of the SOW.

The Contractor will not have access to DHS information systems. The Contractor will perform the work under this acquisition on the Contractor's own system(s).

The Contractor will not have recurring access to Government facilities. Contractor and/or subcontractor employee access to CUI or government facilities will be limited to U.S. Citizens and lawful permanent residents. The Contractor will adhere to all DHS S&T record retention policies (as described in DHS/S&T-001 Research, Development, Test and Evaluation System of Records).

L. 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 Section 508 Requirements for Technology Services (include in the SOW, PWS, or SOO)

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.

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.

3. When developing or modifying web based and electronic content components, except for electronic documents and non-fillable forms provided in a Microsoft Office or Adobe PDF format, the Contractor shall demonstrate conformance to the applicable Section 508 standards (including WCAG 2.0 Level A and AA Success Criteria) by conducting testing using the DHS Trusted Tester for Web Methodology Version 5.0 or successor versions, and shall ensure testing is conducted by individuals who are certified by DHS on version 5.0 or successor versions (e.g. "DHS Certified Trusted Testers"). The Contractor shall provide the Trusted Tester Certification IDs to DHS upon request. Information on the DHS Trusted Tester for Web Methodology Version 5.0, related test tools, test reporting, training, and tester certification requirements is published at https://www.dhs.gov/trusted-tester.

4. Contractor personnel shall possess the knowledge, skills and abilities necessary to address the accessibility requirements in this work statement.

1.2 Section 508 Deliverables

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.

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.

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.

4. **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.

M. EA Compliance.
All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.

- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Architecture Division (EAD) for review, approval and insertion into the DHS Data Reference Model and Mobius.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

N. Cyber-Supply Chain Risk Management (C-SCRM).

a. Definitions

i. Component: a unit defined by the supplier that connects to and functions as part of the product. For software products, a component is a unit of software defined by a supplier at the time the component is built, packaged, or delivered. For hardware, a component is one hardware unit designed to connect to and function as part of a larger product.

ii. End-of-Life (EOL): means that an ICT product has reached the final stage of the product life cycle in which that version of the ICT product will no longer be supported nor manufactured (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

iii. End-of-Support (EOS): means that an ICT product will no longer be supported (e.g., no patches will be developed, no security improvements will be made, and, sometimes, no troubleshooting technical assistance will be offered).

iv. Information and Communications Technology (ICT): encompasses the capture, storage, retrieval, processing, display, representation, presentation, organization, management, security, transfer, and interchange of data and information; includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks).

v. Product: part of the equipment (hardware, software and materials) for which usability is to be specified or evaluated.

b. Original Equipment Manufacturer (OEM) End-use Information and Communications Technology (ICT) Product

i. The contractor shall provide new equipment unless otherwise formally approved by the Government, in writing. The contractor shall provide only Original Manufacturer (OEM) end-use products to the Government. In the event that a shipped OEM product, or part or

component of that product, fails, all replacements must be new (i.e., non-refurbished, not previously used) OEM.

ii. The contractor may provide previously used OEM products only with written Government approval. Such parts shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

c. Accounting of Components in ICT Products

i. The contractor shall provide and maintain a list of components for each product used in performance of the contract, including through subcontracts or other arrangements. This list for each product shall provide the component manufacturer's name, address, state, and/or domain of registration, and, where applicable, the Unique Entity Identifier (UEI) number, for all components comprising the ICT products.

ii. The contractor shall notify the Government when a new contractor/subcontractor/service provider is introduced to the ICT provided on this contract, or when suppliers of components or products are changed. If a software component used in the performance of the contract is updated with a new build or release, the contractor must update the list provided in accordance with (i) above to reflect the new version of the software. This includes software builds to integrate an updated component or dependency.

iii. For software products, the contractor shall provide all OEM software updates, and patches to correct defects, for the life of the product [i.e., until the "End of Life" (EoL) or "End of Support" (EoS)]. Software updates and patches shall be made available to the government for all products procured under this Contract and replaced when End of Support (EoS) is reached.

iv. A contractor using team members in performance of the contract (e.g., subcontractors or other service providers) shall ensure that the standards for the accounting of components in this subsection are met by team members.

d. Supply-Chain Transport

i. The contractor shall use formal, documented and accountable transit, storage, and delivery procedures (i.e., the possession of the end-use product to be delivered is documented at all times from initial shipping point to final destination, and every transfer of the product from one custodian to another is fully documented and accountable) for all information and communication technology (ICT) shipments to fulfill this contract.

ii. The contractor shall maintain all records pertaining to the transit, storage, and delivery of ICT deliverables under this contract through at least 6 months after acceptance and make available for inspection upon request of the Government.

iii. The contractor shall make use of tamper-proof or tamper-evident packaging for all shipments.

iv. The contractor shall provide a packing slip for each container or package with the information identifying the contract or order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the

customer point of contact.

v. The contractor shall provide a shipping notification to the intended government recipient; with a copy transmitted to the Contracting Officer, or other designated representative. This shipping notification shall be provided electronically and identify the contract or order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Changes to Ownership and Control

The Contractor shall immediately notify the Contracting Officer and Contracting Officer's Representative regarding any significant changes to corporate ownership or control from contract award through final delivery or the end of the period of performance. A significant change would be one in which a change occurs in the individuals or entities who, directly or indirectly, either (1) exercises substantial control over an entity, or (2) owns or controls at least 25 percent of the ownership interests of an entity.

L. Points of Contact

University of Nebraska at Omaha POCs are as follows:

COE Director
[redacted]
The University of Nebraska – Omaha Campus
[redacted]

UNO-NCITE may change the individual designated as a POC upon notice to DHS S&T of such change.

DHS S&T Points of Contact are:

DHS Contracting Officer
[redacted]
Department of Homeland Security Office of Procurement Operations
Science and Technology Acquisition Division
245 Murray Lane, SW
Washington, DC 20528
[redacted]

DHS S&T COR
[redacted]
Contracting Officer Representative
Contract Acquisition Program Support (CAPS)
Department of Homeland Security S&T Directorate
[redacted]

DHS S&T PM
[redacted]
Program Manager
Department of Homeland Security S&T Directorate
[redacted]

DHS S&T Invoicing –
U.S. DHS, ICE
Attn: S&T EXD Invoice
Burlington Finance Center
P.O. Box 1000
Williston, VT 05495-1000
[redacted]

DHS S&T may change the individual designated as a POC upon notice to the NCITE/UNO contracting officer of such change.