# DEPARTMENT OF HOMELAND SECURITY (DHS)

## STATEMENT OF WORK (SOW)
## FOR
## *Learning Management Systems Training - Unconscious Bias/Anti-Bullying, End Harassment, and Hostile Work Environment Information*

## 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).

In June 2021, President Biden issued Executive Order (EO) 14035 on Diversity, Equity, Inclusion, and Accessibility (DEIA) in the Federal Workforce. This executive order launched an initiative to cultivate a federal workforce that draws from the full diversity of the nation and advances equitable employment opportunities. This initiative included the requirement to develop a government wide DEIA Strategic Plan that:

- Defines standards of success for diversity, equity, inclusion, and accessibility efforts based on leading policies and practices in the public and private sectors.
- Identifies strategies to advance diversity, equity, inclusion, and accessibility, and eliminate, where applicable, barriers to equity, in federal workforce functions.
- Includes a comprehensive framework to address workplace harassment.
- Promotes a data-driven approach to increase transparency and accountability.

Within CISA, the Office of Equity, Diversity, Inclusion and Accessibility (OEDIA) is responsible for ensuring diversity, equity, inclusion, and accessibility here at CISA. OEDIA aims to further enhance the current workplace DEIA climate, develop more effective programs, and better focus on future initiatives to enhance DEIA for all employees. OEDIA is committed to the EEO protections codified under Title VII of the Civil Rights Act of 1964 and is working to ensure that CISA grows into a shining example of DEIA for the Department and the federal government. Ergo, CISA seeks to build and maintain a respectful workplace by setting expectations and stopping inappropriate conduct before it becomes illegal harassment, and to build a diverse and inclusive culture of respect and dignity by minimizing the impact of bias and stopping bullying through education and guidance from LMS training courses.

### 1.2 SCOPE

The scope of this requirement requires the purchasing of LMS Training-Unconscious Bias/Anti-Bullying, End Harassment and Hostile Work Environment hosted on ~~Media Partners~~Atana Inc. Learning Platforms (MPLP) or CISA's Learning Management Systems (LMS).

## 2.0 SPECIFIC REQUIREMENTS/TASKS

The contractor shall provide CISA access to ~~Media Partners~~Atana Inc's digital licenses for LMS Training for Unconscious Bias/Anti-Bullying and Sexual Harassment Prevention Information hosted on MPLP or CISA LMS.

### 2.1 TASK ONE. *~~Media Partners~~Atana Inc. Custom Library (3 Courses) – Annual License*

- The contractor shall provide CISA with 3,200 digital licenses for ~~Media Partners~~Atana Inc. Custom Library Employee and Manager eLearning – Hosted on MPLP for the following three courses:
    - Course Title and Description: *"Unintentional Still Hurts"*. Overcoming Unconscious Bias (Understanding Bias, Recognizing Hidden Biases and Microaggressions, Speaking Up/Proactive Leadership).
    - Course Title and Description: *"How Was Your Day"*. Minimize the impact of harassment, End Harassment, and Stop Bullying.
    - Course Title and Description: *"In This Together"* Risk of offensive language & Jokes, Rules when attracted to someone at work, the human cost of gossip, legal definition of hostile work environment perception vs. intent and who wins and losses.

### 2.2 TASK TWO. *Respectful Supervisor: Integrity and Inclusion eLearning – SCORM*

- The contractor shall provide CISA with 400 digital licenses for Respectful Supervisor: Integrity and Inclusion eLearning – Hosted on MPLP.
    - Respectful Supervisor: Integrity and Inclusion (Understand Your role in preventing harassment and discrimination, be aware of Unconscious bias and Micro-inequities, don't be a Bully).

### 2.3 TASK THREE. *Provide Annual Digital License*

- Provide CISA with one (1) Annual Digital License.

## 3.0 DELIVERABLES

**The following are proposed deliverables for this purchase order:**

| ITEM | SOW REFERENCE | DELIVERABLE / EVENT | DUE BY | DISTRIBUTION |
|---|---|---|---|---|
| 1 | 2.1 | Media Partners Custom Library (3 Courses) – Annual License | Within 5 Days after Award | COR |
| 2 | 2.2 | Respectful Supervisor: Integrity and Inclusion eLearning – SCORM | Within 5 Days after Award | COR |

| ITEM | SOW REFERENCE | DELIVERABLE / EVENT | DUE BY | DISTRIBUTION |
|---|---|---|---|---|
| 3 | 2.3 | Annual Digital License Fee | Within 5 Days after Award | COR |

**3.1 DELIVERY INSTRUCTIONS FOR LICENSES**
Delivery shall be made no later than 5 days after award.
The contractor shall deliver all items in the following manner:

***Electronic Delivery***

Contractor shall deliver all items to the following email address: Lisa.danquah@cisa.dhs.gov

**4.0 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.

**4.1** 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.

**4.2** The COR will have 10 business days to review deliverables and make comments. The Contractor shall have 3 business days to make corrections and redeliver.

**4.3** 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.

**5.0 OTHER APPLICABLE CONDITIONS**

**5.1 SECURITY**

Contractor access to CISA Sensitive Information, systems, networks and reoccurring access to CISA facilities is not required under this SOW; therefore, contractor employees will not 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. 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 )If provided by the government to the contractor, is marked in such a way to place a reasonable person on notice of its sensitive nature;
(2) Is designated "sensitive" in accordance with subsequently adopted homeland security information handling requirements."

**5.2 PERIOD OF PERFORMANCE**

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

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

**5.3 SECTION 508 COMPLIANCE**

Section 508 of the Rehabilitation Act (classified to 29 U.S.C. § 794d) requires that when Federal agencies develop, procure, maintain, or use information and communications technology (ICT), it shall be accessible to people with disabilities. Federal employees and members of the public with disabilities must be afforded access to and use of information and data comparable to that of Federal employees and members of the public without disabilities.

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

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the Contracting Officer and a determination will be made according to DHS Directive 139-05, Office of Accessible Systems and Technology, dated November 12, 2018, and DHS Instruction 139-05-001, Managing the Accessible Systems and Technology Program, dated November 20, 2018, or any successor publication.

**5.3.1 Section 508 Requirements for Technology Products**

**Section 508 applicability to Information and Communications Technology (ICT):** ~~Media Partner~~Atana Inc. Digital Licenses

**Applicable Exception:** N/A **Authorization #:** N/A

**Applicable Functional Performance Criteria:** All functional performance criteria in Chapter 3 apply to when using an alternative design or technology that results substantially equivalent or greater accessibility and usability by individuals with disabilities than would be provided by conformance to one or more of the requirements in Chapters 4 and 5 of the Revised 508 Standards, or when Chapters 4 or 5 do not address one or more functions of ICT.

**Applicable 508 requirements for electronic content features and components** (including but not limited to electronic training materials): All requirements in E205 apply, including all WCAG 2.0 Level A and AA Success Criteria apply as specified in E205

**Applicable 508 requirements for software features and components** (including but not limited to Web, desktop, server, mobile client applications)

**Applicable 508 requirements for hardware features and components:** Does not apply

**Applicable 508 requirements for support services and documentation:** All requirements in Chapter 6 apply

### 5.3.2 Section 508 Requirements for Technology Services

1. When providing Platform as a Service (PaaS) or Software as a Service (SaaS), the contractor shall ensure services conform to the applicable Section 508 standards (including the requirements in Chapter 5 for software and WCAG Level A and AA Level 2.0 success criteria for web and software. When the requirements in Chapter 5 do not address one or more software functions, the Contractor shall ensure conformance to the Functional Performance Criteria specified in Chapter 3.) The agency reserves the right to request an Accessibility Conformance Report (ACR) for PaaS and SaaS offerings. The ACR should be created using the Voluntary Product Accessibility Template Version 2.2 508 (or later). The template can be located at https://www.itic.org/policy/accessibility/vpat

2. When providing cloud hosting services (Infrastructure as a Service, Platform as a Service, Software as a Service, etc.) the Contractor shall ensure user administrative screens, dashboards and portals used to configure, and monitor cloud services conform to the Section 508 standards.

3. The Contractor shall ensure cloud hosting services shall not reduce the level of Section 508 conformance for ICT migrated by DHS to the cloud hosting environment.

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

### 5.3.3 Section 508 Deliverables

1. **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 the instructions provided in the template, including an explanation of the validation method used as a basis for the conformance claims in the report.

## 5.4 DHS ENTERPRISE ARCHITECTURE 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 Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- 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.

## 5.5 DHS GEOSPATIAL INFORMATION SYSTEM TERMS AND CONDITIONS

All implementations including geospatial data, information, and services shall comply with the policies and requirements set forth in the DHS Geospatial Information Infrastructure (GII), including (but not limited to) the following:

- All data built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Data Reference Model.
- All software built to the GII, whether adopted or developed, shall be submitted to the government for review and insertion into the DHS Technical Reference Model.

## 5.6 EPEAT AND ENERGY STAR LANGUAGE

"All hardware procured directly or in support of this action must meet applicable and appropriate Electronic Product Environmental Assessment Tool (EPEAT) and ENERGY Star standards."

**5.7 DHS CYBER-SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) TERMS & CONDITIONS**

a. The Offeror understands and agrees that the Government retains the right to cancel or terminate the Contract, if the Government determines that continuing this solicitation presents an unacceptable risk to national security.

b. "Gray-Market" Equipment

i. The Offeror shall provide only new equipment unless otherwise expressly approved, in writing, by the DHS Contracting Officer. Offerors shall provide only Original Equipment Manufacturer (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

ii. The Offeror shall be excused from using new OEM (i.e., "gray market", "previously used") components only with formal Government approval, in writing, from the DHS Contracting Officer. Such components shall be procured from their original source and shipped only from the manufacturer's authorized shipment points.

iii. All equipment obtained by the Offeror on behalf of the Government will need to be provided to OIG OCIO for review to validate requirements and approved Contractors by DHS.

c. Hardware and Software Requests

iv. The contractors supply the Government hardware and software will provide the manufacturer's name, address, state, and/or domain of registration, and the DUNS number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state, and/or domain of registration and DUNS number of those suppliers must be provided.

v. Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors will perform due diligence to ensure that these standards are met.

vi. The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

1. For software products, the Offeror shall provide all OEM software updates to correct defects for the life of the product (i.e., until the "End of Life (EoL)"). Software updates and patches shall be either: made available to the government for all products procured under this Contract, replaced upon End of Support (EoS) is reached, or formally waived (in writing) by the DHS Contracting Officer.

d. Supply-Chain Transport

vii. Offerors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented

at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill Contract obligations with the Government.

viii. All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the Contract, the period of performance, or one calendar year from the date the activity occurred.

ix. This transit process shall minimize the number of times in route components undergo a change of custody and make use of tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

x. All records pertaining to the transit, storage, and delivery shall be readily available for inspection by any agent designated by the U.S. Government as having the authority to examine them.

xi. The Offeror is fully liable for all damage, deterioration, or losses incurred during shipping and handling, unless the damage, deterioration, or loss is due to the Government.

xii. The Offeror shall provide a packing slip which shall accompany each container or package with the information identifying this solicitation number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact.

xiii. The Offeror shall send a shipping notification to the intended government recipient; with a copy transmitted via email to the Contracting Officer, or designated representative. This shipping notification shall be sent electronically and will state this solicitation number, the order number, a description of the hardware/software being ship (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

e. Notifications

xiv. The Offeror shall notify DHS Contracting Officer, COR and the Office of the Chief Information Officer and the DHS component Chief Information Officer through the Enterprise Security Operations Center (ESOC) directly of any suspected or potential violations of Section 889 of the National Defense Authorization Act (NDAA) for Information Communications Technology (ICT) at NDAA_Incidents@hq.dhs.gov.

f. Foreign Equities

The Offeror shall immediately notify the DHS Contracting Officer, COR that will report to the Office of the Chief Security Officer (OCSO) or cognizant component personnel security office regarding any changes to corporate foreign ownership, control, or influence.

## 6.0 CONTRACTOR FURNISHED PROPERTY

The Contractor shall furnish all facilities, materials, equipment and services necessary to fulfill the requirements of this contract.

## 7.0 INVOICES AND PAYMENT PROVISIONS

Invoices shall be prepared per Section VII, Contract Clauses; Paragraph A. entitled "FAR CLAUSES INCORPORATED BY REFERENCE," FAR Clause 52.232-25 Prompt Payment, and FAR Clause 52.232-7, Payments under Time and Materials and Labor-Hours. In addition to invoice preparation as required by the FAR, the Contractor's invoice shall include the following information:

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.

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.