**PART I. REQUIREMENT OWNER INFORMATION**

1. Emergency: This requirement is in support of an Emergency Declaration

{projectOverview.emergencyDeclaration ? `Yes` : `No`}

2. Requirements information.

Requirements Title: {projectOverview.title}

Brief Description of the Requirement:

{projectOverview.scope}

3. Mission Owner Agency/Organization Information:

Agency: {organization.agency}

Organization: {organization.name}

4. Task Order Contracting Officer Representative (TO COR) nominee.

Name: {contacts.cor.name}

Email: {contacts.cor.email}

Phone Number: {contacts.cor.phoneNumber}

Department of Defense Activity Address Code (DoDAAC): {contacts.cor.dodaac}

{IF contacts.acor}

Alternate TO COR nominee.

Name: {contacts.acor.name}

Email: {contacts.acor.email}

Phone Number: {contacts.acor.phoneNumber}

Department of Defense Activity Address Code (DoDAAC): {contacts.acor.dodaac}

{END-IF}

**PART II. REQUIREMENT INFORMATION**

1. Do you have a current contract for the same effort:

{ currentContract.exists ? `Yes` : ` No`}

{IF currentContract.exists}

Incumbent Contractor Name: {currentContract.incumbentContractorName}

Contract Number: {currentContract.contractNumber}

Task Order Number: {currentContract.taskOrderNumber}

Contract/Task Order expiration date: {currentContract.contractExpiration}

{END-IF}

2. Does your market research indicate an exception to the fair opportunity process (Federal Acquisition Regulation (FAR) 16.505(b)(2))?

{exceptionToFairOpportunity.includes(`YES`) ? `Yes, a Justification & Approval is required` : `No`}

3. Recurring Requirement. Will this be a future recurring requirement?

{periodOfPerformance.recurringRequirement ? `Yes` : `No`}

4. What is the requested Period of Performance (PoP) of the requested task order?

{popPeriods}

Is there a REQUESTED PoP start date?

{periodOfPerformance.popStartRequest ? `Yes` : `No`}

{IF periodOfPerformance.popStartRequest}

{periodOfPerformance.timeFrame}: {periodOfPerformance.requestedPopStartDate}

{END-IF}

5. Contract Type

{IF contractType.firmFixedPrice}

Firm-Fixed-Price (FFP)

{END-IF}

{IF contractType.timeAndMaterials}

Time-and-Materials (T&M) (Other than Travel)

T&M Justification:

{contractType.justification}

{END-IF}

6. Business Associate Agreement (BAA). Does the contract action provide for definition of a Business Associate who may be involved in but not limited to design or development (in whole or in part) of the system, and/or for creating, receiving, transmitting, managing, and disposing of Protected Health Information (PHI)?

{sensitiveInformation.baaRequired ?

`Yes, a HIPAA BAA is required between the Mission Owner and the business associate to provide assurance that the business associate will appropriately safeguard such e-PHI. Business associates must also obtain BAAs from their subcontractors.` : `No`}

7. Public Disclosure of Information. Does your work statement (Description of Work) and/or DD254 contain information that, if released, would be harmful to the Government?

{sensitiveInformation.potentialToBeHarmful ? `Yes, include the name and address of your FOIA coordinator below` : `No`}

{IF sensitiveInformation.potentialToBeHarmful}

FOIA Coordinator:

Name: {sensitiveInformation.foiaContact.fullName}

E-Mail Address: {sensitiveInformation.foiaContact.email}

Physical Address:

{sensitiveInformation.foiaContact.address}

{END-IF}

{IF organization.agency === `Defense Information Systems Agency (DISA)`}

**PART III. DISA CHIEF INFORMATION OFFICER (CIO) CERTIFICATION**

***(REQUIRED ONLY FOR DISA MISSION OWNERS)***

1. Clinger-Cohen Act (CCA) Compliance: CCA compliance is required for all Programs that acquire Information Technology (IT) per Subtitle III of Title 40, and DoDI 5000.82, April 21, 2020, Clinger Cohen Compliance). This applies to all IT hardware and software acquisitions and acquisition of IT services.

I attest that the DISA CIO has confirmed that this contract action is CCA compliant in accordance with DISA Instruction 630-225.9 in the CCA Confirmation Memo dated November 28, 2022.

2. Data Center Obligation of Funds Compliance: CIO approval required prior to the obligation of funds for data server purchases or other IT items purchased in support of data centers. This is required for accounting and classification.

Not applicable to JWCC as acquisition is not for a Data Center.

3. CyberNetOps Tools Policy Compliance: Per DISA CIO policy, contracts requiring the procurement of a tool supporting Cyber Operations must open an Office of CIO (OCIO) Cyber NetOps Change Request prior to acquiring the new tool or capability. DISA Programs must first utilize existing tools on the OCIO Cyber NetOps Tools baseline list maintained by DISA OCIO to avoid procuring duplicative capabilities.

*Please select the appropriate bullet option below to assist the DISA CIO in verifying or establishing compliance. Delete the options that do not apply. Submit requests for signature to disa.meade.re.mbx.cca-compliance@mail.mil.*

* No, contract does not procure any Cyber NetOps Tools.
* No, contract procures for an existing Cyber NetOps Tool already on the OCIO Cyber NetOps Tools baseline.
* Yes, contract procures a new Cyber NetOps Tool, DISA OCIO Cyber NetOps Change Request attached.
* Yes, contract procures a new Cyber NetOps Tool, DISA OCIO Cyber NetOps Change Request not currently filed.

Program Manager Name:

{contacts.missionOwnerName}

**Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

DISA CIO Certifying Official

**Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**PART IV. MISSION OWNER CERTIFICATION**

{END-IF}

{IF organization.agency !== `Defense Information Systems Agency (DISA)`}

**PART III. MISSION OWNER CERTIFICATION**

{END-IF}

Upon signature of this document, the Mission Owner certifies:

1. The requirement complies with the current Internet Protocol Version 6 (IPv6) Policy as reflected in the IPv6 compliance assessment.

2. The requirement complies with the current DoD Information Enterprise Policy.

3. The requirement does not contain inherently Governmental functions in accordance with FAR 7.5.

Does the Mission Partner certify to the above?

Yes

Mission Partner Name:

{contacts.missionOwnerName}

**Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

{IF organization.agency === `Defense Information Systems Agency (DISA)`}

**PART V. SECTION 508**

{END-IF}

{IF organization.agency !== `Defense Information Systems Agency (DISA)`}

**PART IV. SECTION 508**

{END-IF}

Mission Owners must confirm whether the below Section 508 requirements apply to this acquisition.

*Electronic Content*

*Technical Criteria:*

*E205.1 General - Electronic content shall comply with E205.*

*E205.2 Public Facing - Electronic content that is public facing shall conform to the accessibility requirements specified in E205.4.*

*602 Support Documentation*

*603 Support Services*

*302 Functional Performance Criteria*

*Software*

*Exceptions:*

*E207.1 General - Software that is assistive technology and that supports the accessibility services of the platform shall not be required to conform to the requirements in Chapter 5.*

*E207.2 WCAG Conformance - Software that is assistive technology and that supports the accessibility services of the platform shall not be required to conform to E207.2.*

*Non-web software shall not be required to conform to the following four Success Criteria in WCAG 2.0: 2.4.1 Bypass Blocks; 2.4.5 Multiple Ways; 3.2.3 Consistent Navigation; and 3.2.4 Consistent Identification.*

*Non-Web software shall not be required to conform to Conformance Requirement 3 Complete Processes in WCAG 2.0.*

*Functional Performance Criteria:*

*301.1 Scope - The requirements of Chapter 3 shall apply to ICT where required by 508 Chapter 2 (Scoping Requirements), 255 Chapter 2 (Scoping Requirements), and where otherwise referenced in any other chapter of the Revised 508 Standards or Revised 255 Guidelines.*

*302.1 Without Vision - Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that does not require user vision.*

*302.2 With Limited Vision - Where a visual mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited vision.*

*302.3 Without Perception of Color - Where a visual mode of operation is provided, ICT shall provide at least one visual mode of operation that does not require user perception of color.*

*302.4 Without Hearing - Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that does not require user hearing.*

*302.5 With Limited Hearing - Where an audible mode of operation is provided, ICT shall provide at least one mode of operation that enables users to make use of limited hearing.*

*302.6 Without Speech - Where speech is used for input, control, or operation, ICT shall provide at least one mode of operation that does not require user speech.*

*302.7 With Limited Manipulation - Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that does not require fine motor control or simultaneous manual operations.*

*302.8 With Limited Reach and Strength - Where a manual mode of operation is provided, ICT shall provide at least one mode of operation that is operable with limited reach and limited strength.*

*302.9 With Limited Language, Cognitive, and Learning Abilities - ICT shall provide features making its use by individuals with limited cognitive, language, and learning abilities simpler and easier.*

Are the above Section 508 requirements sufficient for this acquisition?

{sensitiveInformation.section508 ? `Yes` : `No, complete the Accessibility Requirements Tool at app.buyaccessible.gov and insert the applicable procurement language into your Description of Work.`}