Request for Information (RFI)

Defense Counterintelligence and Security Agency (DCSA)
National Center for Credibility Assessment (NCCA)
A/V System Evaluation and Upgrade

1. Description

The Defense Counterintelligence and Security Agency (DCSA) is issuing this Request for Information (RFI) in support of the National Center for Credibility Assessment (NCCA). This RFI is issued solely for market research and planning purposes. It does not constitute a Request for Proposal (RFP), solicitation, or commitment by DCSA to issue an RFP or to award a contract. Responses are voluntary, nor does it obligate the Government, and will not result in reimbursement.

2. Background

The National Center for Credibility Assessment (NCCA) requires a comprehensive technical assessment and engineering design effort across its instructional spaces. The core requirement is to assess the specific hardware currently installed, evaluate the physical space constraints, and verify the exact types and capabilities of the existing A/V equipment. This engineering evaluation is necessary to address system performance gaps within NCCA's current footprint, specifically regarding audio quality in 36 training labs and centralized remote viewing capabilities for 18 isolated "pods" and 2 main classrooms.

The contractor will serve as an expert A/V Design Consultant to provide professional A/V and network design and engineering services. This Phase 1 contract is strictly for design and consultation services. The core requirements are detailed below:

Phase 1 Objective	Description of Contractor Deliverables
On-Site Analysis	Conduct a comprehensive physical and technical audit of the existing A/V equipment, space configurations, and current system architecture.
Course of Action (COA) Briefing	Deliver a technical briefing outlining three (3) viable engineering COAs based on the assessment findings.
Final Implementation Package	Produce a complete, build-ready package (including a Draft PWS, Bill of Materials, and Engineering Drawings) that the Government can utilize for a future Phase 2 Implementation contract.

3. Capability Statement

To assist the Government in determining market capability, responding vendors should provide documentation demonstrating their technical qualifications and experience in the following areas:

Focus Area	Capability & Information Requested
Corporate Experience	Provide summary references for up to three (3) projects of similar scale and complexity completed within the last five (5) years, demonstrating experience with federal or defense-sector enterprise A/V systems.
Industry-Standard Design Credentials	Demonstrate that the proposed Lead System Designer holds recognized, senior-level industry design certifications (e.g., tier-one, independent professional A/V design credentials).
Control System & Architecture Expertise	Demonstrate certified, enterprise-level engineering capabilities with major commercial control systems, including the ability to analyze, program, and evaluate uncompiled system source code to inform design recommendations.
Audio DSP Expertise	Demonstrate certified partnership status and technical expertise in configuring, programming, and calibrating enterprise-grade Digital Signal Processors (DSPs) to resolve complex acoustic and audio-quality issues.

3.1 Company Information

a) Company Name:
b) Commercial and Government Entity (CAGE) Code:
c) Address (including telephone number and email address):
d) Points of contact:
e) Size if business ourusant to North American Industry Classification System (NAICS) Codes:

NAICS Code	NAICS Code Description	Size Standard
541512	Computer Systems Design Services	$34 Million

Based on the above NAICS Code, state whether your company is:

1. Small Business (Yes/No)
2. Women Owned Small Business (Yes/No)
3. Small Disadvantaged Business (Yes/No)
4. 8(a) Certified (Yes/No)
5. HUBZone Certified (Yes/No)
6. Veteran Owned Small Business (Yes/No)
7. Service-Disabled Veteran Small Business (Yes/No)

Vendors that wish to respond to this RFI should send responses via email no later than July 16, 2026 10AM EST to Tracey Fann at tracey.a.fann.civ@mail.mil or Noemi Cordova-Vazquez at noemi.v.cordovavazquez.civ@mail.mil.

4. **Security:**

   Contractor will not have unsupervised access to systems and networks. The contractor shall coordinate with the responsible DCSA Office of the Chief Information Officer (OCIO) or Program staff prior to any visit. The visiting contractor shall be escorted at all times by the responsible DCSA OCIO staff.

   Controlled Unclassified Information (CUI) / Receive, Store, or Generate Controlled Unclassified Information (CUI): Contractor will be provided and will abide by DoD Regulation 5400.7, DoD Freedom of Information Act Program, and DoD 5200.01-M, Information Security Program. Guidance provided under separate cover. In accordance with DoD Instruction 5200.48 (DoDI 5200.48) dated March 6, 2020, Contractors are required to ensure all personnel receive and complete Initial and Annual Refresher CUI education and training and maintain documentation of this training for audit purposes. Initial and Annual Refresher CUI security education, training and awareness on the required topics identified in Section 2002:30 of Title 32 CFR, including protection and management of CUI, to DoD personnel and contractors through the Center for Development of Security Excellence (CDSE).

   Operations Security (OPSEC):

   The contractor shall comply with OPSEC requirements contained in the contract, addendum thereto, or identified herein. The contractor will comply with all security and OPSEC policies, directives, instructions or mandates as directed. OPSEC and other security guidance issued to the Prime Contractor shall also apply to subcontractors working on this effort.

The contractor will ensure compliance with the Agency's OPSEC Policy Statement, Critical Information and Indicators List (CIL), and unclassified document destruction procedures. Items of critical information are those facts, which individually, or in the aggregate, reveal sensitive details about the mission, operation, etc., and thus require protection from adversarial collection or exploitation.

Include OPSEC as part of the security awareness program. The contractor shall be familiar with OPSEC and will be required to take government furnished initial and annual refresher OPSEC training and will be reminded of their continued responsibility to protect sensitive information as directed by DoDM 5205.02. Sensitive unclassified information includes, but is not limited to, agency identified critical information, legacy "For Official Use Only" (FOUO), Controlled Unclassified Information (CUI), Privacy Act of 1974, Personally Identifiable Information (PII), Department of Defense Unclassified Controlled Nuclear Information (DoD UCNI) and company proprietary information.

The contractor shall take the necessary precautions to ensure employees with access to the sensitive and critical information are instructed not to disclose or disseminate any information relating to the conduct and performance of the contract to any individual not authorized to perform on this contract. Assigned personnel shall be knowledgeable of the designated critical information and measures in place to protect it.

For programs protected by a Program Protection Plan (PPP) and have identified Critical Program Information (CPI) and/or Critical Technologies Information (CTI), must be identified and protected in accordance with DoD Instruction 5200.39, CPI Identification and Protection within RDT&E. The contractor shall ensure that any program with CPI or CTI has the corresponding supplements and associated plan, such as an OPSEC plan, approved and in effect in support of the PPP.

The contractor shall comply with OPSEC content review policies within the Agency. A content review is an evaluation of all information, to include all CUI, intended for release outside the control of the organization or release to the public. OPSEC focuses on identifying and protecting the organization's unclassified information that may individually or in the aggregate lead to the compromise of classified information and sensitive activities. The contractor will ensure that these reviews are conducted according to agency guidance in accordance with mandates from DoDD 5205.02E, DoD OPSEC Program, DoDM 5205.02-M, DoD OPSEC Program Manual, DoDI 5230.09, Clearance of DoD Information for Public Release, DoDI 5230.29, Security and Policy Review of DoD Information for Public Release, DoDI 5400.04, Provision of Information to Congress, DoDM 5400.07, DoD FOIA Program, and DoDI 8170.01, Online Information Management and Electronic Messaging.

Further OPSEC guidance may be obtained by the Prime contractor contacting the OPSEC PM by group e-mail: dcsa.quantico.dcsa-hq.mbx.operations-security@mail.mil.

All programs and materials developed at government expense during the performance period of this contract are the property of the US Government.

Contractor personnel shall utilize US Government or official company e-mail for transmitting official US Government business. Official US Government business shall NOT be transmitted via personal, private, and/or commercial e-mail accounts, i.e., YAHOO, HOTMAIL, GMAIL, JUNO, AOL, COMCAST, KNOLOGY, VERIZON, etc.