Identity, Credential, and Access Management (ICAM)
Request for White Papers
Project Number: DISA-OTA-20-R-ICAM

DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

Other Transaction Authority (OTA)

Request for White Papers (RWP)

Project Number	DISA-OTA-20-R-ICAM
RWP Title	Identity, Credential, and Access Management (ICAM)
Issued by	Defense Information Systems Agency (DISA) Other Transaction (OT) Agreement Team
White Papers Due Date/Time (Suspense)	November 5, 2019 no later than 2 PM Central Standard Time (CST)
Submit White Papers To	disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, vanessa.a.mccollum.civ@mail.mil, and craig.j.carlton.civ@mail.mil.

Note: Please advise DISA as soon as possible via email to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil if your organization intends to submit a White Paper to DISA in response to this RWP.

Amendment 0002 is issued to respond to vendor questions and make updates to the Request for White Papers. All changes to the RWP are highlighted in yellow. The due date for White Papers is changed to November 12, 2019 at 4PM EST.

Amendment 0001 is issued to extend the White Paper due date to November 19, 2019 at 12PM EST.

SECTION 1—OVERVIEW/DESCRIPTION

1.1 PURPOSE

This request for White Paper (RWP) is being issued to conduct research, development, and testing activities associated with Identity, Credential, and Access Management (ICAM) activities. This request meets the statutory requirements of Other Transaction Authority (OTA) (10 U.S.C. §2371) for the development and deployment of a DoD Enterprise Identity Service that will create a single user record, consolidating all pertinent data associated with the individual under one account, and automatically deleting such accounts when they are no longer required. The objective will be to establish a federated identity service for DISA, its mission partners, non-CAC holders (such as authorized guests and visitors), and non-person entities that mitigates current inefficiencies, facilitates strong authentication to current state-of-the-art cloud services, provide authorization services with role-base access, and enables audit of users and resources; using non-traditional defense contractor solutions per 10 USC §2302(9), which defines a non-traditional defense contractor as "an entity that is not currently performing and has not performed, for at least one year preceding the solicitation of sources by the DoD for the procurement or transaction, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards prescribed pursuant to 41 USC §1502 and the regulations implementing such section."

The project involves technology that exists in the marketplace, but not in the breadth, scope, and bandwidth that would be capable of integrating the entire DoD Enterprise and all of its unique systems and requirements, and ensuring their seamless integration and interoperability in the manner and at the level that this mission-critical federated identity effort requires. In the latter regard, it is very much a prototype.

ICAM capabilities will enhance the security and integrity of DoD information systems that serve and protect warfighters and the military and civilian personnel who support them. ICAM does so proactively rather than reactively, by restricting unauthorized access to systems and information across organizational boundaries, reducing the opportunity for infiltration and violation of DoD enterprise integrity, mitigating inefficiencies and known cyber threats, and maximizing the effectiveness of the ICAM community. Some examples of inefficiencies to be mitigated are the paper DD2875 access request process, ineffective account lifecycle management, lack of visibility into which users have access to what systems, and lack of flexibility to leverage authenticators beyond public key infrastructure (PKI)-based solutions.

1.2 STATEMENT OF NEED

As indicated in "Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors" (HSPD-12), issued August 27, 2004, within and among the agencies of the Department of Defense and their components,

> there are wide variations in the quality and security of identification used to gain access to secure facilities where there is potential for terrorist attacks. In order to eliminate these variations, U.S. policy is to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). This directive mandates a federal standard for secure and reliable forms of identification.

Additionally, Committee on National Security Systems' CNSSD No. 507, "National Directive for Identity, Credential, and Access Management Capabilities (ICAM) on the United States (US) Federal Secret Fabric," dated 24 March 2014, directs "U.S. Government Departments and Agencies that have National Security Systems to establish and manage improved interoperable ICAM capabilities," and Office of Management and Budget (OMB) Memo M-19-17, Enabling Mission Delivery through Improved Identity, Credential and Access Management, issued 21 May, 2019, directs Agencies to establish capabilities aligned to the Federal ICAM Architecture.

As the DoD Enterprise is currently configured, and particularly with reference to its mission partners, mobile platforms, and cloud/AI and other major technology evolutions, the system lacks the ability to identify who or what is accessing the network at any given time, or what resources and data are accessible to such users. The issue persists because DoD does not have an enterprise-wide ICAM capability to centrally monitor, manage, secure, and audit identity, access, and authorization seamlessly across DoD Components and their dynamic and disjointed computing environments.

DoD Combatant Commands/Services/Agencies/Field Activities (CC/S/A/FAs) are currently establishing their own ICAM capabilities in a similar fashion. The resulting challenge faced by DISA and the DoD Chief Information Officer (CIO) is to integrate and monitor data ingress and egress seamlessly between these diverse vendor capabilities, to meet broad enterprise requirements—and more specifically, to provide DoD with the ability to audit who has access to what (and when) across diverse organizational boundaries. DISA's enterprise ICAM effort will also modernize the agency's identity capabilities to streamline the process, and expand its functionality beyond the current identity synchronization, entitlement management, and enterprise directory services, thereby increasing productivity, improving information sharing (and reducing the risks associated with it), enhancing operability, and increasing the timeliness and effectiveness of threat identification and mitigation across the DoD enterprise.

ICAM supports the desired outcomes mandated by the 2018 National Defense Strategy (NDS) Lines of Effort (LOEs) 1, 2, and 3, which require DoD components to:

- Enable information, and provide data sharing for Joint, Interagency, Intergovernmental, and Multinational operations;

- Support reform technology outcomes vis-à-vis mobility, the Cloud, artificial intelligence (AI), and networks;
- Enable threat mitigation by combating the theft and re-use of user credentials, insiders/attribution, social engineering, stale access, and replayable credentials; and
- Dynamically tailor digital access policies as risks evolve and the sharing environment change.

The technical requirement consists of two developmental phases:

- **Technical Phase I** will consist of proposed solution "white papers," and (upon evaluation thereof by the Government) will result in a down-selection to the two or three most promising approaches. The successful candidates will develop preliminary prototypes that will demonstrate functionally critical, software components that are integrated, and functionally validated, to establish interoperability and validated in both vendor and government managed lab environments for initial development and government acceptance testing (GAT). Phase I will conclude prior to the start of Technical Phase II.
- **Technical Phase II** will consist of selection of the best solution, and award of a prototype Other Transaction (OT) agreement to the most successful offeror for Phase II, during which the awardee will develop the ICAM prototype in a production environment for integration with six initial customer applications, and support pre-production/acceptance testing. A successful solution prototype will, at minimum, meet (and ideally, will exceed) the technical criteria set forth in the Request for White Papers (RWP) and the jointly developed Project Work Statement. If the Government elects to adopt the solution thus developed for production, deployment, and sustainment, it may do so under a FAR-based contract or a production OT Agreement.

In support of the DoD Enterprise ICAM, DISA's system enhancements will include:

- **Identity Provider** (IdP) claims-based Centralized Authentication Services for applications, consisting of username and password management, multifactor authentication enablement, and management, and a token provider;
- **Automated Account Provisioning** (AAP) Identity Governance Services, such as User Entitlement Management, business rule auditing and enforcement, account provisioning and de-provisioning based on identity data produced during DoD person-centric activities, such as on and off-boarding, continuous vetting, talent management, and readiness training;
- **Master User Record (MUR)** to enable DoD-wide knowledge, audit, and data rollup reporting of who has access to what systems or applications. Supports identification of insider and external threats, and enables financial management segregation of duties auditability across DoD Component organizations.

- **ICAM Enablement Services**, comprised of Identity Synchronization Services, including a virtual meta directory, data normalization, and ingress/egress identity data synchronization
- **ICAM Integration Services,** provide support to adopt, integrate and deconflict what capabilities are available to application owners at a local level and what is available at the enterprise.

Based on the foregoing, the proposed solution shall provide:

1.2.1. Enterprise Identity Provider (IdP) Access Management Services

DoD-wide shared service to enable authentication to DoD resources using DoD-approved credentials of an appropriate assurance vector issued by DoD, federal interagency, Defense Industrial Base (DIB), and allies when authorized by the system/data owner including:

- Web Access Management/Single Sign-On (SSO)
- Federated Identity Management/SSO
- Authentication & Authorization
- Access Management Application Program Interfaces (APIs)

1.2.1.1. Context-aware security, based on multi-level roles and attributes, such as user identity, device identity, network, authentication type, geographic location, and resource combination.

1.2.1.2. Dynamically-assigned entitlements predicated on user Role-Based Access Control (RBAC) and/or Attribute-Based Access Control (ABAC).

1.2.1.3. Non-Common Access Card (CAC) authentication, single sign-on, and user self-service capabilities

1.2.1.4. Configurable/step-up multi-factor authentication options based on the specific scenario or risk.

1.2.1.5. Identity services for non-Department of Defense Information Network (DoDIN) users and personal devices.

1.2.1.6. Integration with DoD enterprise mobile device management capabilities to ingest device management state data.

1.2.2. Automated Account Provisioning (AAP)

Provides account provisioning and de-provisioning based on identity data produced during DoD person-centric activities (such as on and off-boarding, continuous vetting, talent management, and readiness training), including:

1.2.2.1. Identity Governance and Administration Services

1.2.2.2. Self-Service

1.2.2.3. User-friendly portal for end-user requests

1.2.2.4. Self-service for domain and application owners to maintain control of their identities, and authorizations

1.2.2.5. Delegated Administration

1.2.2.6. Enable tiered structures for multi-level approvals

1.2.2.7. Configurable delegation of approval permissions to local level personnel

1.2.2.8. Automation Workflow Approvals

1.2.2.9. Enterprise Role Definition

1.2.2.10. Integration with downstream DoD Component directories and identity governance tools

1.2.2.11. Audit Role & Compliance Services

- Centralized Audit
- Logging and Monitoring
- Access Certification
- Per-User and Per-Asset Reporting
- Data export to 3rd party tools

1.2.2.12. Fully-automated Federal Identity, Credential, and Access Management (FICAM)/ Federal Information System Controls Audit Manual (FISCAM) compliance reporting for identity and credentials

1.2.3. Master User Record (MUR)

Consists of a data aggregation or distributed query capability of enterprise account entitlements, roles, attributes, and enables DoD-wide knowledge, audit, and reporting of which users have access to what systems or applications at any point in time. Supports identification of internal and external threats, and enables financial management segregation of duties auditability across DoD Component organizations.

The proposed solution shall:

1.2.3.1. Investigate the feasibility and potential scalability of DoD-wide MUR deployment, and identify the sources of identity information

1.2.3.2. Integrate manual data ingest from legacy applications and systems; integrate with applications for automated identity/role data export; and integrate with the provisioning services used by DoD Components

1.2.3.3. Audit privileged and unprivileged accounts

1.2.3.4. Enable insider-threat analytics

1.2.3.5. Provide flexible reporting dashboards and queries for system owners and senior leaders

1.2.4. ICAM Enablement Services

Comprised of Identity Synchronization Services modernization from current DISA Identity Synchronization Services (IDSS), including a virtual meta-directory, data normalization, and ingress/egress identity data synchronization

1.2.4.1. Enable identity aggregation from multiple sources

1.2.4.2. Map and correlate identity information, data/schema de-confliction

1.2.4.3. Create custom views and feeds of identity data

1.2.4.4. Migrate current DISA implemented Microsoft [Forefront] Identity Manager policies and capabilities into solution

1.2.5. ICAM Integration Services

Provide support to adopt, integrate and deconflict what capabilities are available to application owners at a local level and what is available at the enterprise.

Financial management applications are a particular priority for DoD. The Office of the Under Secretary of Defense (Comptroller), OUSD(C), has identified financial management-related applications that are within the initial scope of the ICAM effort. At the time of contract award, the government will specify which application(s) will be selected to integrate with ICAM capabilities.

In Technical Phase I, the Offerors of the two or three best solutions will be required to design and develop a prototype capable of demonstrating and integrating six high priority applications identified by the DoD into the enterprise ICAM services.

Upon successful demonstration and integration, the selected solution(s) will be required to meet follow-on milestones that continue to onboard crucial applications.

In Technical Phase II, one successful Offeror will be required to evaluate and implement recommendations concerning roles to establish and ensure auditable segregation of duties across all on-boarded applications.

SECTION 2—GENERAL SUBMISSION REQUIREMENTS

2.1 FORMATTING

Vendors are solely responsible for all expenses associated with responding to this RWP. White Papers shall follow the format described below. Evaluation and selection of the White Papers will be completed based on criteria in

Section 3—Evaluation ApproachandSection 4. Responding to this RWP does not obligate the Government for costs associated with responding to this notice. The Government reserves the right to cancel this requirement if no White Papers satisfy the criteria contained in Section Evaluation Criteria and/or no funding becomes available.

Subject to the availability of funds, the DISA/Defense Information Technology Contracting Organization (DITCO) at Scott AFB, IL intends to competitively issue this effort as an OTA Agreement in accordance with 10 U.S.C. 2371b. If an OTA is awarded from this subject request, the Agreement is not considered a procurement contract and therefore not subject to the Federal Acquisition Regulation (FAR).

The following **White Paper** formatting requirements apply:

- Times New Roman 10 (or larger) single-spaced, single-sided, 21.6 x 27.9 cm (8.5 by 11 inches);
- Smaller type may be used in figures and tables, but must be clearly legible;
- Margins on all sides (top, bottom, left, and right) should be at least 2.5 cm (1 inch);
- Page limit is fifteen (15) pages, does not include cover sheet and the *Affirmation of Business Status Certification, Rough Order of Magnitude (ROM) Template, Intellectual Property Statement/Agreements/Disclosures*;
- *Italic Red* text with brackets borders (e.g. *[company name]*) indicates areas for entry of information by the vendor. Delete all italicized text, contained within brackets before submittal of the White Paper;
- Page limitations shall not be circumvented by including inserted text boxes/pop-ups or internet links to additional information. Such inclusions are not acceptable and will not be considered as part of the response to Request for White Papers; and

*** * * <u>DO NOT SUBMIT ANY CLASSIFIED INFORMATION</u>. * * ***

A White Paper **Cover Sheet** is required for all submissions, and must include the following:

- OTA Project Number;
- Project Title;
- Company Title/Name of Proposed Effort;
- Date of Submittal;
- Primary point of contact (POC), including name, address, phone and e-mail contact information;
- Total ROM cost for the period of performance through September 2021; and
- Disclosure of Information Statement (section Disclosure of Information.

2.2 MINIMUM ACCEPTABILITY

The Government will evaluate RWP submissions that are deemed as "complete". To be considered "complete" submissions must contain at a minimum the following:

- Cover Sheet (section Formatting;
- Completed Data Rights Assertion Table (Section 3.5.6) (section 3.5.6**Error! Reference source not found.**
- Signed Affirmation of Business Statement (section Affirmation of Business Status Certification
- Address all of the Evaluation Criteria Factors (sub-sections Technical– Participants7).

If the vendor fails to include/address the minimum acceptability requirements (as defined above and throughout the RWP) the White Paper submission will/may be deemed non-compliant and inadequate for further evaluation.

2.3 AFFIRMATION OF BUSINESS STATUS CERTIFICATION

Each participant shall complete the certification below. The certification shall be included as an attachment to the White Paper and will not count toward the page limit. Please note that some sections in the certification may be left blank due to the type of business completing this form (e.g. non-traditional defense contractor).

Please note that in order to be eligible to submit a response to the Request for White Paper (RWP), vendors must meet the requirements outlined in 10 U.S.C Section 2371b(d)(1). Vendors shall explain in their White Paper submissions, not to exceed (NTE) 15 pages, how they will meet these statutory requirements. Failure to provide the required explanation may result in your White Paper not being considered for this OTA effort.

Participant Name	*[Insert Participant Name]*
Proposed North American Industry Classification System (NAICS) Code	*[Insert NAICS Code]*
Industry Size Standard	*[Check one of the following boxes]* **☐ Small ☐ Large ☐ Federally Funded Research & Development Center**
Data Universal Numbering Systems (DUNS) Number	*[Insert DUNS Number]*
Commercial & Government Entity (CAGE) Code	*[Insert CAGE Code]*

Active System for Award Management (SAM) Registration	*[Check one of the following boxes and insert date]* ☐ **Yes** ☐ **No** **Expiration Date:**
Address 1	*[Insert Address Number and Street]*
Address 2	*[Insert suite, office, etc. Number]*
City/State/Zip Code	*[Insert City, State, Zip Code]*
Point of Contact (POC) Name/Title	*[Insert POC Name and Title]*
POC Phone/Email	*[Insert POC Phone and Email]*

[Check one of the following boxes:]

☐ **Nontraditional Defense Contractor (NDC):** A NDC is an entity that is not currently performing and has not performed, for at least the one-year period preceding the issuance of this Request for White Papers by the DoD, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards prescribed pursuant to section 1502 of title 41 of the U.S. Code and the regulations implementing such section. All small businesses are considered NDCs. A small business is a business concern as defined under section 3 of the Small Business Act (15 U.S.C. 632). To be considered a small business for the purposes of this RWP, a concern must qualify as a small business under the size standard for the North American Industry Classification System (NAICS) code, as described at 13 C.F.R. 121.201 and the proposed NAICS code above.

☐ **Traditional Defense Contractor:** A traditional defense contractor is an entity that does not meet the definition of a NDC. Any traditional defense contractors must comply with 10 U.S.C Section 2371b(d)(1)(A-C) in order to be eligible to submit an RWP.

This is to certify that the above is accurate, complete, and current as of *[MM/DD/YYYY]* for DISA-OTA-19-R-ICAM.

Signature (electronic signature is acceptable)	X _____
Name	*[Insert Name of Representative]*
Title	*[Insert Title of Representative]*
Date	*[Insert Date of Signature]*

SECTION 3—EVALUATION APPROACH

The Government will employ a four-phased evaluation approach for the award of the ICAM prototype OTA. An award may be made to the responsible vendor whose offer, conforming to the requirements outlined in the RWP, is determined to be the best overall value to the Government, price, and other factors considered. The evaluation criteria are outlined in sub section **TECHNICAL**—Participants.

Throughout the evaluation, the Government reserves the right, but is not obligated, to ask questions about individual vendor solutions. However, any response to the RWP that does not fully address all requirements will be/can be eliminated from further consideration. This RWP constitutes Phase I of the evaluation, described below.

3.1 PHASE I—WHITE PAPER EVALUATION

The Government will conduct an evaluation of all eligible White Paper(s) submitted in response to this RWP. The White Papers will be evaluated to identify viable solutions. Final selection(s) recommendation(s) will be made by the program management technical lead to the Agreements Officer (AO). After the evaluation of White Paper(s), the Government may select two or three solutions and proceed to the next phase. Any vendor whose solution is not selected will be provided a letter containing a brief explanation for non-selection.

3.2 PHASE II—INITIAL PROTOTYPE OT AGREEMENTS

Upon completion of White Paper evaluations, the Government intends to award two or three prototype OT Agreements to the best candidate solutions. Offerors will be given approximately 45 calendar days and approximately $600K to develop a demonstration of their proposed White Paper solution and develop their concept to IOC. Prior to awarding prototype OT Agreements, the Government will ensure that it is in compliance with 10 USC §2371b(d)(1). The Government will obtain approval from the appropriate approval authority, based on the dollar threshold projected for the prototype OT Agreement. This will be done prior to entering into prototype OT Agreement with a selected vendor.

3.3 PHASE III—ORAL PRESENTATIONS AND SOLUTION DEMONSTRATIONS

The Government will invite the Phase II prototype OT Agreement Vendors to provide oral presentations, which can be conducted in person, via videoconference, or phone. During the presentation, each vendor should be prepared to discuss, in detail, and provide a demonstration of its solution illustrating how the solution meets all of the technical requirements as outlined below in paragraph 3.4.1. After the presentations and demonstrations, the Government will evaluate Vendors' solutions, and determine which Vendor provides the best solution and will proceed to the next acquisition phase.

Any vendor whose solution is not selected will be provided with a brief letter of explanation for non-selection.

3.4 PHASE IV—REQUEST FOR PROJECT PROPOSAL

The Government intends to award one prototype OT Agreement in this Phase. Prior to awarding the prototype OT Agreement, the Government will ensure that it is in compliance with 10 USC §2371b(d)(1). The Government will obtain approval from the appropriate approval authority, based on the dollar threshold projected for the prototype OT Agreement. This will be done prior to entering into prototype OT Agreement with a selected vendor.

The Government will issue a Request for Project Proposal (RFPP) to the selected Vendor. Upon receipt of the RFPP, the Government will conduct evaluations to ensure that the proposed solution meets its technical requirements.

Following technical evaluation of the RFPP, the Vendor will meet with the Government to engage in negotiations. The Government will provide an initial model OT agreement to the Vendor, which will be the Government's opening position for negotiations. Using a collaborative process, the Government and the Vendor will develop a detailed Project Work Statement, negotiate Terms and Conditions, agree on milestones, KPPs and deliverables, and negotiate final price with the Vendor. Once the Government and the selected Vendor reach an agreement, the Agreements Officer (AO) will conduct a pre-award review of the prototype OTA Agreement. Upon the completion of the review, the AO will award a prototype OTA Agreement to the selected Vendor. In the event that the Government is unable to reach an agreement with the initial selectee, the Government may re-evaluate White Paper Responses, oral presentations and solution demonstrations, and make another selection.

3.5 EVALUATION CRITERIA

The overall evaluation will be based on the integrated assessment of the criteria outlined in sub-sections 3.5.1—3.5.7.

Vendors are required to meet all of the evaluation requirements, objectives, and representations. Failure to respond to any of the follow evaluation factors listed below (in sub-sections 3.5.1—3.5.7) may result in elimination from the competition. In addition, the Government has included several templates (e.g., tables, etc.) within several of the evaluation factors outlined below, that identify the minimum level of information that must be included with the final submission. If a vendor fails to include the Government provided templates (identified as required), then such failure may result in the vendor's White Paper submission being deemed non-compliant and inadequate for further evaluation.

3.5.1 TECHNICAL

The Government will evaluate the vendor's technical merit based on the criteria listed below. Solutions will be scored based upon:

3.5.2.1. Inclusion of new and creative solutions in the respondent's proposal that address the unique challenges and complexities of the DoD Enterprise, and demonstrate foresight in anticipation of future needs, emerging risks, and scalability.

3.5.2.2. The ability of the respondent's proposed IDP configuration to provide context-aware security, based on multi-level roles and attributes, such as user identity, device identity, network, authentication type, geographic location, and resource combination

3.5.2.3. The ability of the respondent's proposed IDP configuration to provide configurable/step-up multi-factor authentication options, based on the specific scenario or risk.

3.5.2.4. The ability of the respondent's proposed AAP design to provide integration with downstream DoD Component directories and identity governance tools for centralized account requests.

3.5.2.5. The ability of the respondent's proposed MUR concept to integrate manual data ingest from legacy applications and systems; integrate with applications for automated identity/role data export; and integrate with the provisioning services used by DoD Components

3.5.2.6. The ability of the respondent's proposed MUR concept to provide reporting dashboards and queries for system owners and senior leaders.

3.5.2.7. The ease of use for consumer/user facing services of the respondent's proposed ICAM solution

3.5.2.8. The quality of the respondent's detailed, executable program plan to support and provide outreach to DoD components to onboard to ICAM services, including:

- the estimated level of effort
- the resumes and contingent letters of commitment of [whatever personnel you are considering key]
- a schedule template
- Documented enterprise ICAM architecture in blueprint or process-flow format

For reference purposes, Technical Phase I is the equivalent of NASA's Technology Readiness Level (TRL) 4:

4	Component and/or breadboard validation in laboratory environment.	A low fidelity system/component breadboard is built and operated to demonstrate basic functionality and critical test environments, and associated performance predictions are defined relative to the final operating environment.	Key, functionally critical, software components are integrated, and functionally validated, to establish interoperability and begin architecture development. Relevant Environments defined and performance in this environment predicted.	Documented test performance demonstrating agreement with analytical predictions. Documented definition of relevant environment.

The ultimate ICAM objective will be NASA's TRL 8:

8	Actual system completed and "flight qualified" through test and demonstration.	The final product in its final configuration is successfully demonstrated through test and analysis for its intended operational environment and platform (ground, airborne, or space).	All software has been thoroughly debugged and fully integrated with all operational hardware and software systems. All user documentation, training documentation, and maintenance documentation completed. All functionality successfully demonstrated in simulated operational scenarios. Verification and Validation (V&V) completed.	Documented test performance verifying analytical predictions.

3.5.2 SECURITY

The Government will evaluate the vendor's security approach based on the criteria listed below:

3.5.2.1. NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

3.5.2.2. NIST Special Publication 800-63, Revision 3, Digital Identity Guidelines, June 2017

3.5.2.3. NIST Special Publication 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, February 25, 2019

3.5.3 BUSINESS VIABILITY

The respondent's affirmation of business viability shall be included as an attachment to its White Paper submittal, and will not count toward the page limit. This information will facilitate the Government's assessment as to whether the company has the technical capability and resources to effectively accomplish the work delineated herein. The White Paper submittal will address the following:

3.5.3.1. Describe your company or organization:

- When was it established?
- Who are the principals?
- What is the main focus of your business?
- Who are your firm's primary customers?
- What efforts similar in scope or complexity to the ICAM effort have you successfully performed?
- What is your annual revenue (sales and costs)?
- How many personnel do you employ?

- Do you have the personnel and resources necessary to perform this Agreement in house, or do you anticipate subcontracting some of the work? (If you expect to subcontract, in what area[s] do you expect to need third-party support, and why?)
- Where will the portion of the work to be accomplished at the Contractor's facilities be performed?

3.5.4 SCHEDULE

The Government will evaluate the respondent's proposed schedule/timeline/sprints to include milestones, activities, and deliverables to research, evaluate, test, and deliver a prototype. The multifaceted concept exploration and design approach must demonstrate the respondent's ability to provide the Government with a viable solution that comprehensively and innovatively addresses the requirements and evaluation criteria set forth in Sections 1.2—Statement of Need, and 3.5—Evaluation Criteria, above.

Table 1 — Schedule

Phase	Milestone	Deliverable	Estimated Delivery (Weeks/Months after Event)
	○	○	
	○	○	
	○	○	
	○		

3.5.5 PRICE

The vendor shall submit pricing data utilizing the Government's supplied Rough Order of Magnitude (ROM) Template (i.e., table 3). In accordance with section 3, the Government will fund Technical Phase I (comprised of the research and development of an ICAM solution) at not to exceed $600K for each of the two or three awardees. The ROM shall apply to Technical Phase II (which will entail pre-production development of a prototype), not including the cost of proposal preparation in response to DISA's Request for Project Proposals (RFPP). Failure to include the information described within this section may result in the vendor's entire Price/Cost criteria/factor being deemed non-compliant and inadequate for further evaluation review.

In making a selection, the Government will consider affordability in comparison to the Government estimate, to determine whether the proposed solution is in the best interest of the Government. The Government-provided Rough Order of Magnitude (ROM) Template (Table 3) shall be included as an addendum or appendix to the White Paper, and will not count toward the page limit. The respondent is responsible for verifying that the totals within Table 3 are correctly calculated.

The vendor ROM narrative shall discuss the approach used to estimate the price of accomplishing all requirements. The Vendor shall assume the Government knows nothing about its capabilities or estimating approach.

At a minimum, the ROM narrative shall also include the following cost categories for the ROM:

- **Prime Vendor Labor:** The ROM Narrative shall include the basis for which the estimate labor was calculated (i.e., Generic position titles and estimated rates and hours for those individuals).

- **Sub-Vendor/Consultant Labor:** Provide a list of sub-vendor/consultant effort required to meet the technical approach as described in the white paper and the estimated cost. Include the basis for which the estimated labor was calculated (i.e., Generic position titles and estimated fully burdened hourly rates and hours for those individuals).

- **Material/Equipment:** Provide a list of the materials/equipment required to meet the technical approach as described in the White Paper and the estimated cost;

- **ODCs/Travel:** Provide a list of the other direct costs required to meet the technical approach as described in the White Paper and the estimated costs with basis; Identify any expenses incurred by an employee while those individuals are traveling for business purposes. (e.g., estimated costs for

lodging, transportation, and meals) and identify the basis for how the travel costs were calculated.

Identity, Credential, and Access Management (ICAM)
Request for White Papers
Project Number: DISA-OTA-20-R-ICAM

Table 2 — Rough Order of Magnitude Cost/Price Template

Elements	FY2020	FY2021	Grand Total
Program/Project Management			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2020]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2021]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2020-2021]*
Sub–Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2021]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020-2021]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2021]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020-2021]*
Other Direct Costs (ODCs)/Travel	*[Insert Total Cost for ODCs for Fiscal Year 2020]*	*[Insert Total Cost for ODCs for Fiscal Year 2021]*	*[Insert Total Cost for ODCs for Fiscal Year 2020-2021]*
SUBTOTAL	*[Insert Total Cost for Program/Project Management for Fiscal Year 2020]*	*[Insert Total Cost for Program/Project Management for Fiscal Year 2021]*	*[Insert Total Cost for Program/Project Management for Fiscal Year 2020-2021]*

Concept Exploration			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2020]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2021]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2020-2021]*
Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2021]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020-2021]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2021]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020-2021]*
Other Direct Costs (ODCs)/Travel	*[Insert Total Cost for ODCs for Fiscal Year 2020]*	*[Insert Total Cost for ODCs for Fiscal Year 2021]*	*[Insert Total Cost for ODCs for Fiscal Year 2020-2021]*
SUBTOTAL	*[Insert Total Cost for Concept Exploration for Fiscal Year 2020]*	*[Insert Total Cost for Concept Exploration for Fiscal Year 2021]*	*[Insert Total Cost for Concept Exploration for Fiscal Year 2019-2021]*

Design Prototype			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2020]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2021]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2020-2021]*
Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2021]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020-2021]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2021]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020-2021]*
Other Direct Costs (ODCs)/Travel	*[Insert Total Cost for ODCs for Fiscal Year 2020]*	*[Insert Total Cost for ODCs for Fiscal Year 2021]*	*[Insert Total Cost for ODCs for Fiscal Year 2020-2021]*
SUBTOTAL	*[Insert Total Cost for Design Prototype for Fiscal Year 2020]*	*[Insert Total Cost for Design Prototype for Fiscal Year 2021]*	*[Insert Total Cost for Design Prototype for Fiscal Year 2020-2021]*

Test and Evaluation (T&E)			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2020]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2021]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2020-2021]*
Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2021]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020-2021]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2021]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020-2021]*
Other Direct Costs (ODCs)/Travel	*[Insert Total Cost for ODCs for Fiscal Year 2020]*	*[Insert Total Cost for ODCs for Fiscal Year 2021]*	*[Insert Total Cost for ODCs for Fiscal Year 2020-2021]*
SUBTOTAL	*[Insert Total Cost for T&E for Fiscal Year 2020]*	*[Insert Total Cost for T&E for Fiscal Year 2021]*	*[Insert Total Cost for T&E for Fiscal Year 2020-2021]*

TOTAL ROM COSTS			
Prime Vendor Labor	*[Insert Total Cost for Prime Labor for Fiscal Year 2020]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2021]*	*[Insert Total Cost for Prime Labor for Fiscal Year 2020-2021]*
Sub – Vendor/Consultant Labor	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2021]*	*[Insert Total Cost for Sub-Vendor/Consultant Labor for Fiscal Year 2020-2021]*
Material/Equipment	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2021]*	*[Insert Total Cost for Material/Equipment for Fiscal Year 2020-2021]*
Other Direct Costs (ODCs)/Travel	*[Insert Total Cost for ODCs for Fiscal Year 2020]*	*[Insert Total Cost for ODCs for Fiscal Year 2021]*	*[Insert Total Cost for ODCs for Fiscal Year 2020-2021]*
TOTAL	*[Insert Total Cost of All Elements for Fiscal Year 2020]*	*[Insert Total Cost of All Elements for Fiscal Year 2021]*	*[Insert Total Cost of All Elements for Fiscal Year 2020-2021]*

The Government does not require supporting data to justify the estimated costs (e.g., copies of commercial/market price lists/rates, price history, subcontractor quotes, invoices) with the submission of the White Paper. However, vendors will be required to supply the supporting data in response to the Request for Project Proposal, if selected.

3.5.6 DATA RIGHTS ASSERTION

State whether there are any data rights issues that the Government should be cognizant of moving forward. Specifically, please identify any intellectual property, patents and inventions involved in the proposed solution and associated restrictions on the Government's use of that intellectual property, patents and inventions. The following table shall be presented for all assertions.

Table 3 — Data Rights Assertion

Technical Data/Computers Software/ Patent to be Furnished with Restrictions	Basis for Assertion	Asserted Rights Category	Name of Entity Asserting Restrictions
[Identify the technical data/software/patent to be furnished with restriction]	*[Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government's right should be restricted]*	*[Insert asserted rights category (e.g., limited rights (data), restricted rights (software), government purpose rights, SBIR data rights or specifically negotiated license)]*	*[Insert asserted rights category (e.g., limited rights (data), restricted rights (software), government purpose rights, SBIR data rights or specifically negotiated license)]*

3.5.7 PARTICIPANTS

List all participants (i.e. other vendors), including description of contributions and significance of each participant.

Table 4 — Participants

Participant	Business Status (Check one)	Participant Contribution and Significance to Overall Project
[Insert separate row(s) for each additional participant. Delete row(s) as applicable if Participant is the only participant.]	☐ *Traditional* ☐ *Non-Traditional*	*[Insert detailed, quantifiable description which addresses the following:* • *What is this Participant's significant contribution?* • *Why is this Participant's contribution significant to the overall project?* • *How is this Participant uniquely qualified to provide this significant contribution? (Note: number of years of experience is not deemed a unique qualification.)]*

The facility(ies) where the proposed work is to be performed and the equipment or other Participant property which will be utilized for the prototype include: *[Insert a brief description of facility(ies)/equipment proposed for use on the project]*.

SECTION 4 AWARD

4.1 SELECTION DECISION

2.4 IT IS THE GOVERNMENT'S INTENTION TO NEGOTIATE, SELECT, AND FUND A PROTOTYPE PROJECT AT THE CONCLUSION OF THE FOUR-PHASED EVALUATION APPROACH, DESCRIBED IN AFFIRMATION OF BUSINESS STATUS CERTIFICATION

Each participant shall complete the certification below. The certification shall be included as an attachment to the White Paper and will not count toward the page limit. Please note that some sections in the certification may be left blank due to the type of business completing this form (e.g. non-traditional defense contractor).

Please note that in order to be eligible to submit a response to the Request for White Paper (RWP), vendors must meet the requirements outlined in 10 U.S.C Section 2371b(d)(1). Vendors shall explain in their White Paper submissions, not to exceed (NTE) 15 pages, how they will meet these statutory requirements. Failure to provide the required explanation may result in your White Paper not being considered for this OTA effort.

Participant Name	*[Insert Participant Name]*
Proposed North American Industry Classification System (NAICS) Code	*[Insert NAICS Code]*
Industry Size Standard	*[Check one of the following boxes]* **☐ Small ☐ Large ☐ Federally Funded Research & Development Center**
Data Universal Numbering Systems (DUNS) Number	*[Insert DUNS Number]*
Commercial & Government Entity (CAGE) Code	*[Insert CAGE Code]*
Active System for Award Management (SAM) Registration	*[Check one of the following boxes and insert date]* **☐ Yes ☐ No Expiration Date:**
Address 1	*[Insert Address Number and Street]*
Address 2	*[Insert suite, office, etc. Number]*

City/State/Zip Code	*[Insert City, State, Zip Code]*
Point of Contact (POC) Name/Title	*[Insert POC Name and Title]*
POC Phone/Email	*[Insert POC Phone and Email]*

[Check one of the following boxes:]

☐ **Nontraditional Defense Contractor (NDC):** A NDC is an entity that is not currently performing and has not performed, for at least the one-year period preceding the issuance of this Request for White Papers by the DoD, any contract or subcontract for the DoD that is subject to full coverage under the cost accounting standards prescribed pursuant to section 1502 of title 41 of the U.S. Code and the regulations implementing such section. All small businesses are considered NDCs. A small business is a business concern as defined under section 3 of the Small Business Act (15 U.S.C. 632). To be considered a small business for the purposes of this RWP, a concern must qualify as a small business under the size standard for the North American Industry Classification System (NAICS) code, as described at 13 C.F.R. 121.201 and the proposed NAICS code above.

☐ **Traditional Defense Contractor:** A traditional defense contractor is an entity that does not meet the definition of a NDC. Any traditional defense contractors must comply with 10 U.S.C Section 2371b(d)(1)(A-C) in order to be eligible to submit an RWP.

This is to certify that the above is accurate, complete, and current as of *[MM/DD/YYYY]* for DISA-OTA-19-R-ICAM.

Signature (electronic signature is acceptable)	X _____
Name	*[Insert Name of Representative]*
Title	*[Insert Title of Representative]*
Date	*[Insert Date of Signature]*

Section 3—Evaluation Approach, which best meets the evaluation criteria listed in Sub-Section Evaluation CriteriaThe White Paper selection will be conducted in accordance with Government procedures and the evaluation criteria in Sub-Section Evaluation Criteria. The Government will make a determination whether to:

- Select the White Paper(s), or some portion of the White Paper(s); or,
- Reject the White Paper(s) for further consideration.

The White Paper basis of selection decision will be formally communicated to vendors in writing. Once the selection of the best solution(s) is made, the Government team may proceed to the next phase of the evaluation. At any time during evaluations, the Government may choose to cancel this requirement. In case of cancellation, the Government will not be responsible for any expenses associated with responding to the RWP.

4.2 FOLLOW ON PRODUCTION

The Government intends to award two (2) or three (3) prototype OTAs in Technical Phase I and down-select to one (1) prototype OTA in Technical Phase II. Prior to awarding a prototype OTA, the Government will ensure that it is in compliance with 10 USC §2371b(d)(1). The Government will obtain approval from the appropriate approval authority, based on the dollar threshold projected for the prototype OTA. This will be done prior to entering into the prototype OT with a selected vendor.

Provided that the prototype OTA is successfully completed, the Government may award a follow-on production FAR-based contract or OTA to the participant in the transaction for the prototype project, without further competition. If it is determined that transition activities are in the best interest of the Government, then the Government reserves the right to bilaterally modify the Agreement by adding such activities. Prior to award of the production contract or transaction, the Government will ensure that it is in compliance with 10 USC 2371b(f). In addition, the Government will again obtain approval from the appropriate approval authority, based on the dollar threshold projected for the production FAR-based contract or production OTA.

SECTION 5—ADDITIONAL INFORMATION

5.1. DOCUMENTATION CLASSIFICATION

Vendors shall not submit any documentation that is classified as “Confidential,” “Secret,” or “Top Secret” throughout the evaluation process. This includes, but is not limited to, submission of White Papers, Project Proposals, Project Work Statements, etc.

5.2. DISCLOSURE OF INFORMATION

White Papers, Project Proposals, PWS, etc. containing data that is not to be disclosed to the public for any purpose or used by the Government except for evaluation purposes shall include the following sentences on the cover page:

"This white paper includes data that shall not be disclosed outside the Government, except to non-Government personnel for evaluation purposes, and shall not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than to evaluate this submission. If, however, an agreement is issued to this Company as a result of -- or in connection with – the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent agreed upon by both parties in the resulting agreement. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets *[Respondent: insert numbers or other identification of sheets]."*

5.2.1 DATA SHEET MARKINGS

Marking requirements specify that data be "conspicuously and legibly" marked with a protective legend that identifies the OTA number, contractor's name and address, and the submittal date, along with the warning "*Use or disclosure of data contained on this sheet is subject to restriction"* on the title page of any restricted data sheets.

5.3. ANALYTICAL AND LABORATORY STUDIES

It is generally desired that active research and development (R&D) is underway for concepts submitted under this effort. Active R&D includes analytical studies and laboratory studies to physically validate the analytical predictions of separate elements of the technology, as well as software engineering and development. The Government is requesting information on any current or ongoing analytical or laboratory studies related to ICAM solutions. Any information related to ongoing efforts shall be included as an attachment to the White Paper and will not count toward the page limit.

5.4. RECORDS, FILES, AND DOCUMENTATION

All physical records, files, documents, and work papers, provided and/or generated by the Government and/or generated for the Government in performance of this OTA, maintained by the vendor which are to be transferred or released to the Government, shall become and remain Government property and shall be maintained and disposed of as applicable. Nothing in this section alters the rights of the Government or the vendor with respect to patents, data rights, copyrights, or any other intellectual property or proprietary information as set forth in any other part of this RWP (including all clauses that are or shall be included or incorporated by reference into the prototype OTA). The AO may at any time issue a hold notification in writing to the vendor. At such time, the vendor may not dispose of any Government data or Government-related data described in the hold notification until such time as the vendor is notified in writing by the AO, and shall

preserve all such data in accordance with Agency instructions. The vendor shall provide the AO within ten (10) business days of receipt of any requests from a third party for Government-related data. When the Government is using a vendor's ICAM solutions, the vendor shall provide the Agency with access and the ability to search, retrieve, and produce Government data in a standard commercial format.

5.5. SECURITY CLEARANCES

The vendor is responsible for providing personnel with appropriate security clearances to ensure compliance with Government security regulations. The vendor shall fully cooperate on all security checks and investigations by furnishing requested information to verify the vendor employee's eligibility for any required clearance.

The vendor's proposed solution (e.g., data, integration with supporting DoD infrastructure, architecture, etc.) will determine the personnel security clearance requirements for the prototype effort. The Government will provided additional details regarding the required security clearances in the RFPP.

5.6. DATA STORAGE

To protect against seizure and improper use by non-United States (U.S.) persons and government entities, all data stored and processed by/for the DoD must reside in a facility under the exclusive legal jurisdiction of the U.S. The vendor will be required to maintain all government data that is not physically located on DoD premises[1] within the 50 States, the District of Columbia, and outlying areas of the U.S., unless otherwise authorized by the responsible Government, as described in DoDI 8510.01[2] and the DoD Cloud Computing Security Requirements Guide[3].

If Government data is co-located with the non-Government data, the vendor shall isolate the Government data in an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Government personnel identified by the Agreements Officer, and without the vendor's involvement. The vendor shall record all physical access to the cloud storage facilities and all logical access to the Government data. This may include the entrant's name, role, purpose, account identification, entry and exit time. Such records shall be provided to the Agreements Officer or designee in accordance with the agreement or upon request to comply with federal authorities.

[1] A facility (building/container) or IT infrastructure is On-Premises if it is physically on DoD owned or controlled property. That is, it is within the protected perimeter (walls or "fence line") of a DoD installation (i.e., Base, Camp, Post, or Station (B/C/P/S) or leased commercial space) which is under the direct control of DoD personnel and DoD security policies.
[2] https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf
[3] https://iasecontent.disa.mil/cloud/Downloads/Cloud_Computing_SRG_v1r3.pdf

5.7. LAW ENFORCEMENT

The vendor acknowledges and affirms that United States (U.S.) Federal law enforcement officials do not need a warrant or a subpoena to access Government data on any system or media employed by the vendor or its sub-vendors, other partners, or allies, to deliver or otherwise support the contracted service for the U.S. Government, subject to requirements for access to classified information and release thereof, if applicable. As specified by the Agreements Officer, the vendor shall provide immediate access to all Government data and Government-related data impacting Government data for review, scan, or conduct of a forensic evaluation and physical access to any contractor facility with Government data.

5.8. NOTIFICATION

The vendor shall notify the Government Security Contacts (Disa.meade.bd.mbx.sd-security-managers@mail.mil), and the AO within 60 minutes of any warrants, seizures, or subpoenas it receives, including those from another Federal Agency that could result in the loss or unauthorized disclosure of any Government data. The vendor shall cooperate with the Government to take all measures to protect Government data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.

5.9. VENDOR INCURRED EVALUATION COSTS

The costs associated with participating in Phases I through III, to include White Paper(s) preparation and submission, are not considered an allowable charges and should not be included within the ROM or any pricing information.

5.10. EXPORT CONTROLS

Research findings and technology developments arising from the resulting White Paper may constitute a significant enhancement to the national defense and to the economic vitality of the United States. As such, in the conduct of all work related to this effort, the recipient will comply strictly with the International Traffic in Arms Regulation (22 CFR 120-130), the National Industrial Security Program Operating Manual (DoD 5220.22-M) and the Department of Commerce Export Regulation (15 CFR 730-774).

SECTION 6—RESPONSES

Questions should be addressed to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, vanessa.a.mccollum.civ@mail.mil, and craig.j.carlton.civ@mail.mil. Please provide any questions, in writing, to the attention of Ms. Vanessa McCollum and Mr. Craig Carlton, no later than ***October 25, 2019 at 2 PM CST***. The Government reserves the right to not answer questions submitted after this time. Any submissions that are received after the close of the solicitation period will receive no further consideration.

The response to this RWP is due no later than ***November 5, 2019 at 2 PM CST***. The responses should be emailed to disa.scott.ditco.mbx.pl84-other-transaction-authority@mail.mil, vanessa.a.mccollum.civ@mail.mil, and craig.j.carlton.civ@mail.mil.