

Broad Agency Announcement (BAA)

N00039-10-X-0001

Space and Naval Warfare Systems Command, PMW 750

**Maritime Patrol and Reconnaissance Forces (MPRF) Intelligence Surveillance
Reconnaissance (ISR) Enhancements through an Enterprise Expeditionary
Operations Architecture (MEEOA)**

TABLE OF CONTENTS

1. PURPOSE..... 3
2. MPRF PROGRAM BACKGROUND..... 4
3. MEEOA REQUIREMENTS 8
4. ADMINISTRATIVE INFORMATION 12
5. SELECTION PROCESS INFORMATION 13
6. APPLICATION AND SUBMISSION INFORMATION 16
7. ELIGIBILITY INFORMATION 17
8. AGENCY CONTACTS..... 17
9. STAGE 1 NOTIFICATION 17
10. ADDITIONAL INFORMATION..... 18

APPENDICES:

Appendix A [Certification and Accreditation Regulations: Information Assurance Rules and Regulations: Required IA Capabilities Support](#)

Appendix B [Relevant Experience Form](#)

TABLES:

Table 1 [MPRF Expeditionary Missions](#)

Table 2 [MEEOA Communications Bandwidth Requirements](#)

FIGURES:

Figure 1 [MTOC Mission Support Cycle Functional Flow](#)

Figure 2 [Essential Expeditionary Enterprise Services](#)

Figure 3 [MTOC Net-Centric System Communications Description](#)

Broad Agency Announcement (BAA)

N00039-10-X-0001

Space and Naval Warfare Systems Command, PMW 750

Maritime Patrol and Reconnaissance Forces (MPRF) Intelligence Surveillance Reconnaissance (ISR) Enhancements through an Enterprise Expeditionary Operations Architecture (MEEOA)

1. PURPOSE

The Space and Naval Warfare Systems Command (SPAWAR), on behalf of the Program Executive Office – Command, Control, Communications, Computers, Intelligence (PEO C4I), Carrier and Air Integration Program Office (PMW 750) is investigating Maritime Patrol and Reconnaissance Forces (MPRF) Intelligence Surveillance Reconnaissance (ISR) enhancements through an Enterprise Expeditionary Operations Architecture (MEEOA) with the potential for incorporation into a future Program of Record. PMW 750 is interested in receiving technical papers that describe a proposed architecture or prototype solution. After review of the papers, PMW 750 may award a single contract with an estimated value of \$2 - 3 million for an architecture/prototype.

The goal of the MEEOA is to expand existing MPRF ground support capabilities with an architecture and supporting data strategy that provides simultaneous/consolidated and/or integrated Unclassified, Secret Collateral, TOP SECRET, Secret Compartmentalized Information (SCI), Special Access Program (SAP) and Combined Enterprise Regional Information Exchange System (CENTRIXS) Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) support to the MPRF Mission Support Cycle while retaining the following characteristics:

- Small footprint
- Transportable
- Modular
- Scaleable
- Tailorable
- Interoperable
- Services Oriented Architecture (SOA)
- Comprised of components that are certified by NSA or in the process of NSA certification.

The MEEOA will provide a war-fighting capability to the Navy to support all facets of expeditionary warfare, including littoral, open ocean, and land operations. MEEOA ground-based C4ISR systems are vital to the Navy's war-fighting vision, supporting the Sea Power 21 pillars of Sea Strike, Sea Basing, and Sea Shield, and will be critical enablers of Naval Warfare through the Common Operational Picture (COP), Global Information Grid (GIG) and Service Oriented Architecture (SOA). In this capacity,

MEEOA systems and facilities will support operations in a range of mission areas including deterring, fighting, and winning major theater wars; Overseas Contingency Operations (OCO); regional conflicts; supporting overseas presence; and conducting rapid power projections, crisis response, disaster relief, and support across the full range of military operations supporting national interests.

The MEEOA will greatly enhance the Maritime Tactical Operations Center's (MTOC's) capabilities to quickly assess cross domain information to support well-informed decisions. The ability to process consolidated classified security domain C4ISR information and/or integrate C4ISR information normally separated in exclusive classified security domains will prove extremely valuable in formulating precise, well-informed decisions, courses of action, and promulgation of ISR information to supported Commanders and GIG.

2. MPRF PROGRAM BACKGROUND

The MPRF consists of all current and planned MPRF platforms (Patrol Aircraft (P-3C), Patrol Aircraft (P-8A), Broad Area Maritime Surveillance (BAMS), Electronic Patrol Aircraft (EP-3E/EPX), Littoral Surveillance and Reconnaissance System (LSRS)/Advanced Airborne Sensor (AAS)/Tactical Operations Center (TOC)/ MTOC, MPRF Wings), the MPRF Task Force Commanders (CTF-57, CTF-67, CTF-72), and MPRF Task Group Commander (CTG).

C4ISR information and data of differing classification levels utilized and produced by MPRF platforms is presently handled, processed, and stored within physically separate, independent classified material system domains and enclaves, which are certified and accredited to handle the highest level of information and data required by and produced by each distinct MPRF platform.

At the present time, C4ISR information protected by differing classified security domains cannot, without manual or limited system sanitization capability, be consolidated, integrated, shared, or migrated down to warfighters working within lower classification domain enclaves. The present architecture inhibits timely access, fusion, and assessment of intelligence across multiple classification domain sources by MPRF watch officers and operational and tactical commanders.

C4ISR information handled, processed, and stored by the MPRF falls under the following security classification domains:

UNCLASSIFIED: Information of, relating to, or being official matter not requiring the application of security safeguards.

CONFIDENTIAL: Containing information, the unauthorized disclosure of which poses a threat to national security.

SECRET Collateral: Containing information, the unauthorized disclosure of which poses a serious threat to national security.

TOP SECRET: Information whose disclosure could result in grave danger to the national security; the highest of the three commonly known levels of national security classification, the others being CONFIDENTIAL and SECRET. The handling of TOP SECRET information is subject to the provisions of DOD 5200.1-R, Information Security Program Regulation.

SCI: All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentalization have been or will be formally established. (These controls are over and above the provisions of DOD 5200.1-R).

SAP: A sensitive program, approved in writing by a head of agency with original TOP SECRET classification authority that imposes need-to-know and access controls beyond those normally provided for access to CONFIDENTIAL, SECRET, or TOP SECRET information. The level of control is based on the criticality of the program and the assessed hostile intelligence threat. The program itself may be an acquisition program, an intelligence program, or an operations and support program. Security policy and procedures for storing, processing, and communicating classified DoD SAP information in information systems (IS) is governed by JAFAN 6-3.

2.1 MPRF OPERATIONS

MPRF forces must maintain themselves in a high state of deployability and general readiness. Expeditionary operations require the versatility and adaptability to respond effectively, without a great deal of preparation time, to a broad variety of circumstances. An expedition involves the deployment of military forces to the scene of a crisis or conflict, with their requisite support, some significant distance from their home bases. The term “expeditionary” also implies austere conditions and support. This does not mean that an expeditionary force is necessarily small or lightly equipped, but that it is no larger or heavier than necessary to accomplish the mission and contains the required equipment, systems, manning, and physical structure. An expeditionary capability, as it pertains to MPRF C4ISR support, emphasizes standards for the physical structures, technical systems, and the manpower and practices required to support the deployed MPRF Enterprise, to include Joint, Allied, and Coalition Forces.

MPRF employs the CENTRIXS for coalition interoperability and support, currently offering information flow strictly via multiple versions of CENTRIXS networks to individual coalition partners. Security technology to allow separate, simultaneous communities of interest across common network transport is the key to future coalition networking.

MPRF units typically forward-deploy personnel and equipment and conduct operations until they achieve their objectives and then redeploy. The types of missions that MPRF forces may conduct are described in Table 1.

Table 1. MPRF Expeditionary Missions

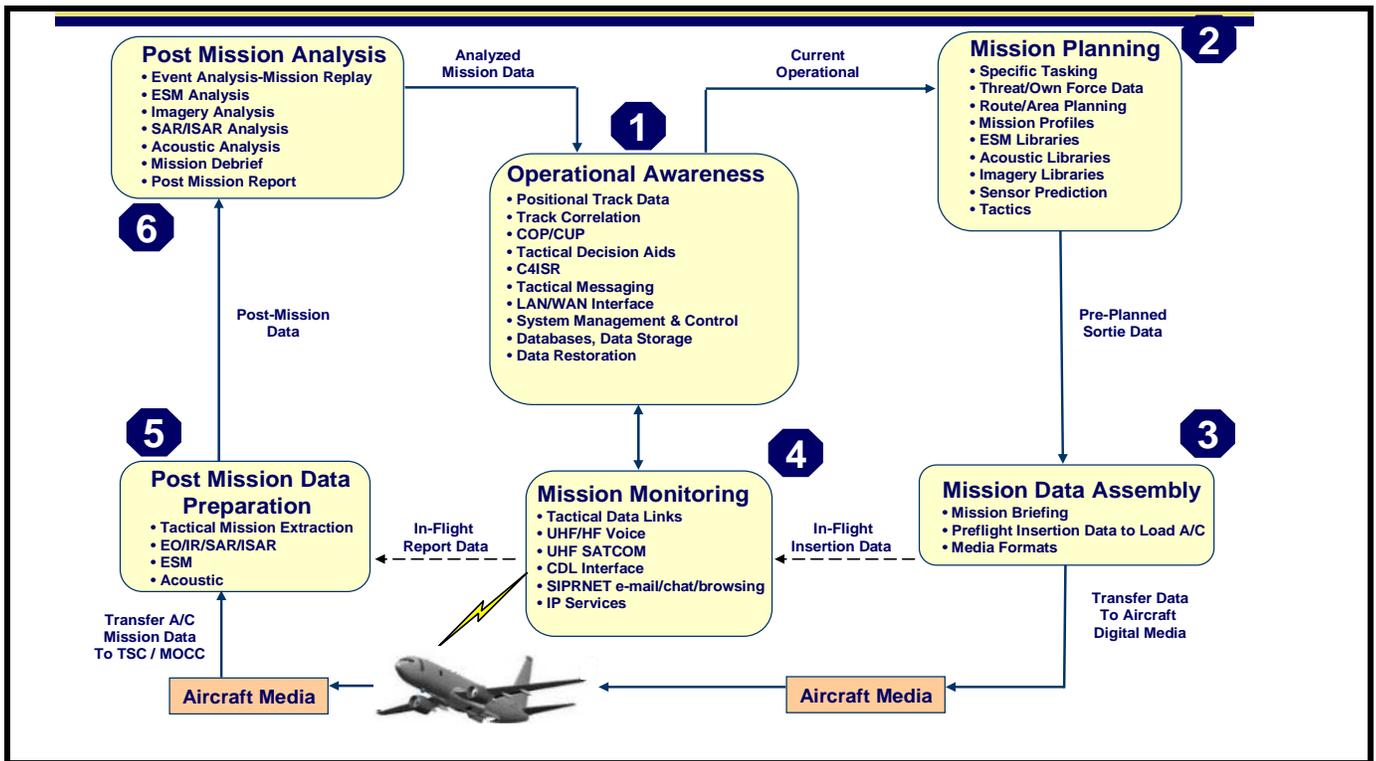
MISSION TYPES	
Direct Maritime Support	Envisioned any time that MPRF forces are tasked to employ MPRF expeditionary capabilities at the behest of a deployed Maritime Commander during military operations.
Associated Maritime Support/Independent Operations	Envisioned any time that MPRF forces are tasked to employ MPRF expeditionary capabilities and/or MPRF Commander capabilities at the behest of any Maritime Commander / Joint Commander that cannot / will not directly control MPRF mission execution.
Joint Air Operations	Envisioned any time that MPRF forces are tasked to employ MPRF expeditionary capabilities at the behest of any Joint Air or Land Component Commander during MPRF mission execution.
Military Operations Other Than War (MOOTW)	Envisioned any time that MPRF forces are tasked to employ MPRF expeditionary capabilities across a range of military operations short of war that are in direct support of civil and federal authorities.
SPECIFIC MISSION AREAS	
Maritime and Littoral Surveillance	Support for armed reconnaissance (over-water and over-land)
Anti-Surface Warfare (ASUW)	Over-the-Horizon Detection, Classification, and Targeting (OTH/DCT)
Mine Warfare (MIW)	Information Operations
Counter-Drug (CD)	Undersea Warfare (USW)
Power Projection	Search and Rescue (SAR)
Special Operations (SPECOPS)	Strike Warfare (STW)
Mission/Warfare Readiness Training	

In the current operational environment, there is limited information sharing between the separate systems and enclaves processing C4ISR information of differing security classification domains. Each enclave requires its own physical facility, (i.e. Sensitive Compartmented Information Facilities (SCIF), manpower, generators, environmental control units, spare parts, etc.)

The MTOC presently provides the MPRF deployable C4ISR system support infrastructure for the SECRET Collateral and below security domains only. MTOCs contain a full spectrum detachment of MPRF C4ISR mission cycle support equipment which can be transported within theater by either military or commercial airlift. When available, MTOCs are dependent upon base hotel services for shelter, power, and

environmental control. Self-sustaining MTOCs presently depend upon three 30-kilowatt generators for organic power. The MTOC C4ISR systems presently support the MPRF Mission Support Cycle to include Operational Awareness, Mission Planning, Mission Data Assembly, Mission Data Extraction, Post Mission Analysis and Expeditionary Operations. The MTOC Mission Support Cycle Functional Flow is illustrated in Figure 1. A block diagram of the MTOC 2.0 system is available on the Net-Centric Enterprise Solutions for Interoperability (NESI) website at: <http://nesipublic.spawar.navy.mil>. (See Section 4, Administrative Information, for information on how to obtain access to the NESI website).

Figure 1. MTOC Mission Support Cycle Functional Flow



2.2 MTOC DEPLOYMENT SITES AND MANNING

MTOC detachments normally deploy to Secondary Deployment Sites (SDS) and Expeditionary Deployment Sites (EDS). MPRF SDSs are *prepared* forward echelon operations sites. MTOC detachments to SDS support scaleable C4I extension or full autonomous MPRF operations for as long as dictated by mission requirements. MPRF EDSs are *unprepared* forward echelon operations sites. MTOC detachments to EDS also support scaleable C4I extension or full autonomous MPRF operations for as long as dictated by mission requirements. MTOC detachments also provide an organic manpower component comprised of three C4I watch teams totaling 26 personnel, including one intelligence specialist.

3. MEEOA REQUIREMENTS

The Government is seeking MPRF ISR Enhancements with supported data strategy enhancements through an Enterprise Expeditionary Operations Architecture or a prototype system that can perform the following functions:

- 1) Support multiple security enclaves associated with MPRF operations within an expeditionary operational employment model
- 2) Minimize impacts of MPRF Manpower (number of personnel and personnel and skill-sets) training, and administration (security clearances)
- 3) Support a "take only what you need" construct; e.g. operations at the lowest security level required for mission support
- 4) Utilize components that are NSA certified or are in the process of NSA certification
- 5) Integrate and enable existing mission support cycle functions

At a minimum, proposed architectures/prototypes shall have the capability to perform both single security enclave and multiple security enclave consolidated C4ISR processing. Consolidated C4ISR processing is the ability to process information from all classified security domains (Unclassified, Secret, Collateral, Top Secret, SCI, SAP) processed by the same C4ISR system in a Multiple Independent Levels of Security (MILS) framework based on the concepts of separation and controlled information flow; implemented by separation mechanisms that ensure the total security solution cannot be bypassed, can be evaluated, and is always invoked and tamperproof. Architectural concepts/prototypes must comply with the Certification and Accreditation (C&A) requirements contained in Appendix A and must be ground based, employ a SOA, have a small footprint, be modular, utilize components that are NSA certified or in the process of NSA certification, and leverage existing MTOC organic C4ISR, mobility/facility and power and environment support capabilities.

Ideally, the proposed architecture/prototype shall perform integrated C4ISR processing. Integrated C4ISR processing is the ability to process information from all classified security domains (Unclassified, Secret, Collateral, Top Secret, SCI, SAP) from a single terminal. Information is processed by the same C4ISR system in a Multi-level Security (MLS) framework, permitting simultaneous access by users with different security clearances and need-to-know while preventing users from obtaining access to information for which they lack authorization. MLS will allow for the integration and sharing of information across all classified security domains. Architectural concepts prototypes must comply with the C&A requirements contained in Appendix A, be ground based, employ a SOA, have a small footprint, be modular, utilize components that are NSA certified or in the process of NSA certification, and leverage existing MTOC organic C4ISR, mobility/facility and power and environment support capabilities.

Consolidated and Integrated Solutions must be capable of:

- Sanitizing classified information for integration and access on the GIG

- Sanitizing classified information for integration and access on the Common Tactical Picture (CTP)
- Sanitizing classified information for integration and access on the UNCLASSIFIED Common Operational Picture (UCOP).

MEEOA capabilities (for either Consolidated or Integrated C4ISR processing) must take into consideration the following design characteristics:

Small footprint: Minimum Space, Weight, and Power (SWaP), minimal required environmental control equipment, minimal C4ISR equipment and ancillary equipment, minimal manpower, etc.

Transportable: Designed to be rapidly deployable and capable of supporting MPRA operations at Secondary Deployment Sites (SDS) and Expeditionary Deployment Sites (EDS); they may perform as extensions of TOCs or as independent C4I nodes. MEEOA frameworks incorporate features to support their transportability such as portable antenna systems, electrical generators and power distribution systems.

Modular: Composed of separate, independent modules that can be rearranged, replaced, combined, or interchanged easily.

Scaleable: MEEOA frameworks will be deployed in a manner that seamlessly extends MPRF C4I from the rear-echelon shore environment into forward areas of maritime execution. MEEOA extensions into the area of responsibility can be scaled to the anticipated task load, the requirements of supported commanders, and the aircraft mission requirements. MEEOA systems will incorporate the capability to adapt hardware or software applications and Mission Capability Packages (MCP) to accommodate changing work loads.

Tailorable: Although MEEOA frameworks may be equipped with comprehensive mission support capabilities, the modular systems design will allow for determination and selection of the right mix and sequencing of system capabilities and MCPs to support and accomplish the MPRF mission. In the MEEOA context, this includes the ability to take only the security enclaves needed and to be able to operate at the lowest security level required.

Interoperable: Ability to access, manipulate, and exchange information between multiple disparate systems, such as in the current C4ISR operational environment.

SOA: The underlying structure supporting communications between services. SOA defines how two computing entities, such as programs, interact in such a way as to enable one entity to perform a unit of work on behalf of another entity. Service interactions are defined using a description language. Each interaction is self-contained and loosely coupled, so that each interaction is independent of any other interaction.

NSA Certifiable: MEEOA frameworks shall utilize components that are certified by NSA or in the process of NSA certification.

MEEOA systems will be absorbed into the MTOC structure and will be supported by the existing MTOC manpower structure. MEEOA will receive, exploit, and post MPRA tactical data using enterprise services that enable critical interfaces to the GIG and other SOAs such as:

- Global Command & Control System – Maritime (GCCS-M)
- Net-Centric Enterprise Services (NCES)
- Community of Interest (COI) portals
- Distributed Common Ground System - Navy (DCGS-N)

Communications among all participating forces must be seamless and integrated and must comply with the communication bandwidth constraints listed in Table 2.

Table 2. MEEOA Communications Bandwidth Requirements

Common Interface	MEEOA (Mbps)	
	Threshold	Objective
SIPRNET	10.240	51.200
JWICS	N/A	1.544
NIPRNET	5.120	10.240
VTC / DVS-G	0.384	0.384
CENTRIXS	0.256	0.512
DSN	0.128	0.512
Access to Commercial Voice	0.128	0.256
Subtotal	16.256	64.648
Subtotal (x1.45 for redundancy)	23.571	93.740
ADDITIONAL CIRCUITS NOT INCLUDED IN CALCULATIONS		
	Threshold	Objective
TCDL (LOS)	45.00	45.00
GBS	24.00	24.00

As the C4ISR element of the MPRF, the ground-based MEEOA framework will provide and/or facilitate essential enterprise services (Figure 2) to MPRF and other Naval, Joint, Allied, and Coalition forces. The MEEOA will also utilize the present MTOC

communications capabilities, with the addition of requisite crypto systems required for classified information transmission and receipt. The present MTOC Net-Centric System Communications Description is illustrated in Figure 3.

Figure 2. Essential Expeditionary Enterprise Services

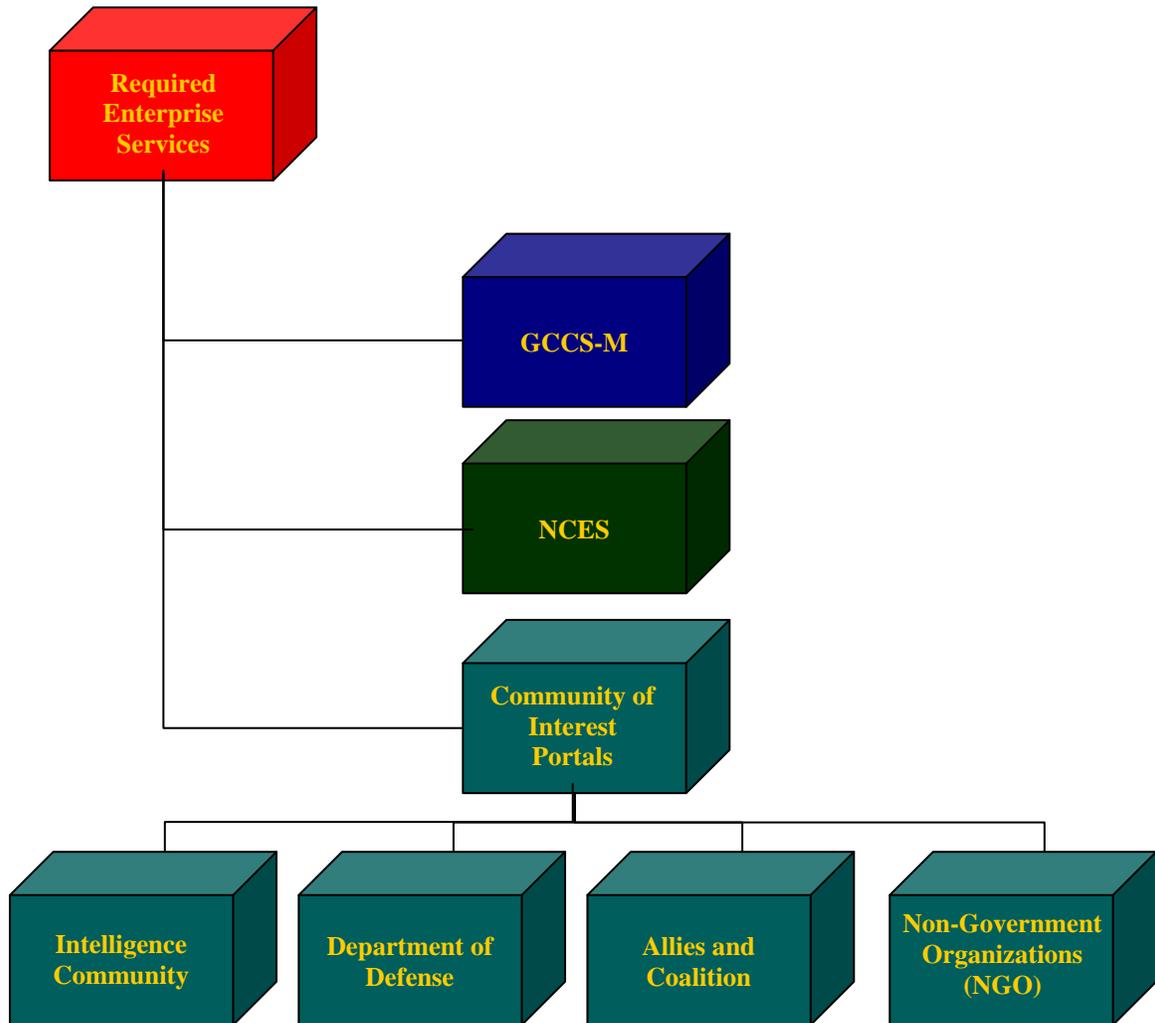
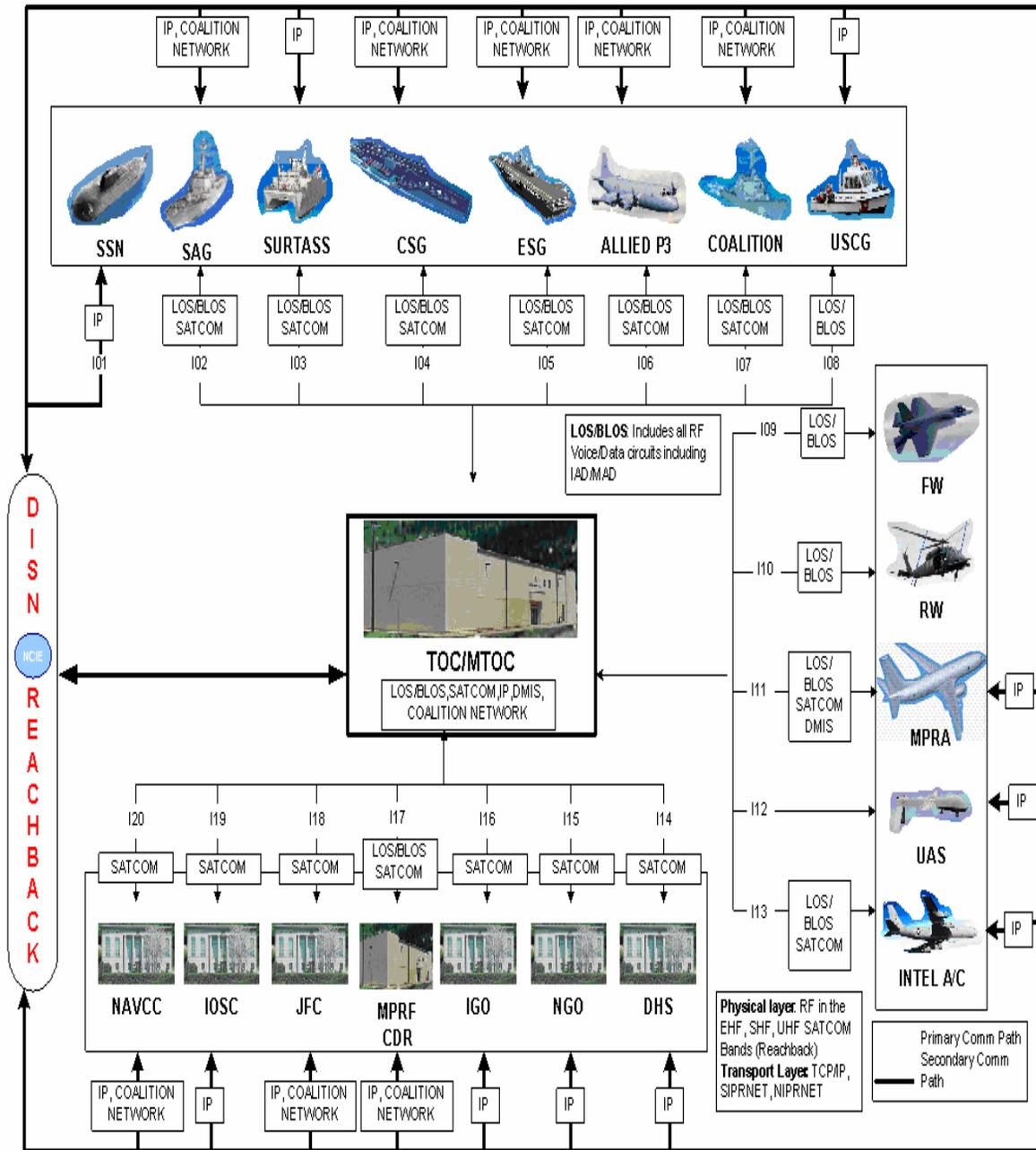


Figure 3. MTOC Net-Centric System Communications Description



4. ADMINISTRATIVE INFORMATION

4.1 Access to NESI Site

The Government has posted the MTOC 2.0 System Block Diagram to NESI for industry review in support of the MEEOA BAA. NESI access is limited to U.S. Department of Defense (DoD) contractors who possess a valid DoD or ECA-issued PKI certificate.

To request access to the secured website, Respondents must sign and return the Non-Disclosure Agreement (NDA) posted on the SPAWAR e-commerce site entitled “MEEOA BAA Bidder’s Repository NDA.” An e-mail address and phone number must be provided for each requested user to Patricia Ponce-Feliu at patricia.poncefeliu@navy.mil and Frederick Renz at frederick.renz@navy.mil. Respondents may request access for up to two users. U.S. DoD contractors who do not have a valid DoD or ECA-issued PKI certificate should contact LCDR Scott Murray at scott.murray@navy.mil for additional information.

The Government will provide instructions on how to access the secured site to the approved requested users after the required NDAs are received and the company’s status as a U.S. DoD contractor is verified. Additional or updated documentation may be posted to the secured site after the initial documents are posted; therefore, it is the responsibility of any interested party to monitor the site for additional postings.

4.2 Notification of Use of Contractor Support

Contractor support personnel from Booz Allen Hamilton shall assist the Scientific Review Team for administrative purposes only and will not be used in analyzing or reviewing proposals, answering technical questions, writing draft reports, providing comments to evaluators, or any other tasks requiring the rating or scoring of the proposal itself.

Responses to this BAA MUST clearly state that permission is either granted, or not granted, to allow the contractor support personnel identified access to the Respondent's technical papers and any resulting SOW and cost proposal. Should such permission be denied the evaluation will be conducted without the contractor support identified. Respondents are encouraged to execute a Proprietary Data Protection Agreement (PDPA) with Booz Allen Hamilton. The point of contact for the company is listed below:

Company	Point of Contact
Booz Allen Hamilton	Rick Burroughs (burroughs_richard@bah.com)

5. SELECTION PROCESS INFORMATION

The BAA evaluation will be conducted in two-stages, as described below. Stage 1 includes receipt, evaluation, and possible selection of a technical paper; Stage 2 includes a request for a detailed Statement of Work (SOW) and cost proposal to support award of a contract based on the technical paper.

5.1 Stage 1 Process

Stage 1 is receipt, evaluation, and selection of a technical paper. BAA Respondents will submit technical papers addressing the requirements in Section 3 above.

Evaluation Criteria for Stage 1

Technical papers will be evaluated against the following criteria, which are listed in descending order of importance:

1. Relevance of proposed architecture/prototype to MEEOA requirements identified in Section 3 and identification of technical risks.
2. How the proposed architecture/prototype considers and utilizes capabilities identified on the Unified Cross Domain Management Office CD Baseline document.
3. Technical Data Rights restrictions. The Government will consider any restrictions to the Government's rights in intellectual property to be delivered under any contract resulting from this BAA. In addition, respondents shall also provide a specific description of any hardware/software licenses required to implement their MEEOA architecture/prototype, and indicate whether those licenses will be provided to the Government as part of a deliverable item under any contract resulting from the Stage 2 process.
4. How the Respondent's proposed architecture/prototype employs SOA, Maritime Data Models, open architecture tenets, data strategy, and complies with Industry and Government standards.
5. Relevant experience / past performance.
6. Rough Order of Magnitude (ROM) Cost and preliminary schedule for research and development of a prototype/architecture.

Technical Data Rights for Intellectual Property

Respondents to this BAA shall identify all aspects of the intellectual property (technical data, hardware, and software) that the Respondent plans to generate, develop, and/or deliver to the Government with less than Government Purpose Rights in the event that their technical paper is selected for the Stage 2 process. Respondents shall follow the format under DFARS 252.227-7017 to assert any specific restrictions to the Government's rights in intellectual property (technical data, hardware, and software) to be delivered under the resulting contract. If no restrictions are intended, the Respondent should state "None." In the event that the Respondent does not assert any restrictions, the default presumption will be that the Government has Government Purpose Rights to all intellectual property (technical data, hardware, and software) developed under the resulting contract.

Respondents must include all documentation establishing their ownership or possession of appropriate licensing rights to all patented inventions (or inventions for which a patent application has been filed) utilized under their proposals. Where a patent application has been filed but has not yet been made available to outside organizations and contains

proprietary information, Respondents may provide only the patent number, inventor name(s), assignee names (if any), filing date, filing date of any related provisional application, and a summary of the patent title.

Relevant Experience / Past Performance

Using the format provided at Appendix B, Relevant Experience Form, Respondents shall provide relevant experience information on current contracts performed by the Respondent for contracts of similar scope and effort relevant to the requirements of this BAA. This data shall be submitted for no more than three (3) of the most current and relevant contracts. Current is defined as a contract performed within the last five (5) years. Relevant is defined as providing architecture and data strategies for Unclassified, Secret Collateral, Top Secret, SCI, SAP, and CENTRIXS C4ISR systems similar in nature and scope to the TacMobile program.

Respondents shall submit Contractor Performance Assessment Reporting System (CPARS) or Past Performance Information Retrieval System (PPIRS) reports for those contracts provided as relevant experience, for each year of contract performance. Respondents whose relevant past performance information is not located on the automated systems shall provide contract numbers, Government or commercial contract points of contact, phone numbers, and e-mail addresses.

5.2 Stage 2 Process

If the Government determines that a proposed area of research and the approach described in the technical paper is relevant to the MEEOA effort, the selected Respondent will be invited to submit a detailed Statement of Work (SOW) and a cost proposal within 30 calendar days of notification by the Contracting Officer. The Government reserves the right to request a SOW and cost proposal for all or a portion of the selected technical paper.

Statement of Work (SOW)

The SOW will translate the concept described in the technical paper into activities and tasks leading to the development of a MEEOA architecture or prototype. The SOW shall be written in a severable fashion to allow the Government to periodically assess progress and determine whether additional funds will be provided to continue research and development efforts.

The proposed SOW will be incorporated as an attachment to the resultant contract without any proprietary restrictions. All proposed contract deliverables shall be clearly identified.

Cost Proposal

The cost proposal shall contain cost estimates sufficiently detailed for meaningful evaluation, including cost details for proposed subcontractors. For estimating purposes, the selected Respondent should assume a contract award date of 16 June 2010. The cost proposal must include the total cost of the project by major task and must correspond to the schedule/period of performance provided in the technical paper.

Required information for cost proposal:

- a. Direct labor. Identify all required labor categories, labor hours, and direct labor rates.
- b. Estimate of material and operating costs.
- c. Costs of equipment, based on most recent quotations and broken down in sufficient detail for evaluation.
- d. Travel costs and time, and the relevance to stated research and development objectives.
- e. Publication and report costs.
- f. Subcontract costs and type (portion of work to be subcontracted and rationale).
- g. Consultant fees (indicating daily or hourly rate) and travel expenses; include a description of the nature of a need for any consultant's participation.
- h. Overhead rates.
- i. Other direct costs.

6. APPLICATION AND SUBMISSION INFORMATION

6.1 Technical Paper Format

Technical papers must cite the BAA number and the topic name. Technical papers shall be no longer than 25 pages (not to exceed ten pages of administrative information to include a cover page, relevant experience and past performance, and ROM cost estimate). CPARS/PPRIS Reports do not count towards the page limitation. A page is defined as an 8 1/2 x 11-inch paper, single-sided, one-inch margins, and a typeface of 10-pitch.

6.2 Time and Date of Submission

Technical papers must be submitted electronically by 10:00 a.m. PST on 1 February 2010 and shall be unclassified.

6.3 Electronic Submission

Respondents shall register in the SPAWAR E-Commerce Central (E-CC) and select their own passwords in order to submit their technical papers, and if selected for Stage 2, SOW and cost proposal. Respondents are required to read the "Submitting a Proposal?" guide on the SPAWAR E-CC website. For information about electronic submission, please visit the SPAWAR E-CC at <https://e-commerce.sscno.nmci.navy.mil>.

Respondents shall submit their technical papers, and if selected for Stage 2, SOW and cost proposal, electronically to SPAWAR in accordance with the instructions contained in this provision. Respondents shall submit their signed documentation as either scanned "TIFF" or "PDF" documents (which shall be created using Adobe Acrobat Version 4.01 or greater) except for the Stage 2 cost proposal, which shall be an MS Excel document.

All documents shall be submitted electronically via the SPAWAR E-Commerce Central (SPAWAR E-CC).

Each electronic file shall be clearly marked with the BAA number, Respondent's name, and topic. File names must begin with the word "MEEOA," followed by an underscore ("_") and the Respondent's company name (Example: "MEEOA_XYZ Inc.doc" would be used for a paper from Company XYZ Inc in a Word document (.doc) format). This file-naming convention will permit systematic cataloging and distribution of the papers for evaluation.

Electronic proposal files shall not contain classified data. Proposal files may be compressed (zipped) into one, self-extracting file entitled "PROPOSAL.ZIP" using WinZip version 6.3 or greater.

Proposals submitted electronically will be considered "late" unless the Respondent completes transmission of the entire proposal, including all attachments, prior to the due date and time for receipt of proposals.

7. ELIGIBILITY INFORMATION

All responsible, potential Respondents from academia and industry are eligible to submit technical papers. SPAWAR encourages proposals from Black Colleges and Universities, Minority Institutions (including Hispanic Serving Institutions and Tribal Colleges and Universities) and minority researchers, as well as Small Businesses, HUBZone Small Businesses, Small Disadvantaged Businesses, Veteran-Owned Small Businesses (including Service-Disabled Veteran-Owned Small Businesses), and Women-Owned Small Businesses. However, no portion of this BAA is set aside for a specific group.

8. AGENCY CONTACTS

All questions regarding this BAA shall be directed to the Contract Specialist, Patricia Ponce-Feliu, email: patricia.poncefeliu@navy.mil, with a copy to the Contracting Officer, Frederick Renz, email: frederick.renz@navy.mil. No hard copy version of this BAA will be made available. Questions shall be submitted no later than 4 January 2010 and will be answered by 15 January 2010.

9. STAGE 1 NOTIFICATION

Respondents will receive notification approximately six (6) weeks following completion of the Stage 1 evaluation process. The Government reserves the right to select all or some portion of a single technical paper for Stage 2. The Government also reserves the right to cancel the BAA and not award a contract after receipt of technical papers. The Government may incrementally fund any award issued under this BAA. The Government provides no funding for direct reimbursement of technical paper development costs. Technical papers (and any other material) submitted in response to this BAA will not be returned.

Following completion of the Stage 1 evaluation, the selected Respondent will be invited to submit a SOW and cost proposal (Stage 2) within 30 calendar days of notification by the Contracting Officer. **No debriefings of technical paper evaluations will be provided.**

10. ADDITIONAL INFORMATION

10.1 Organizational Conflict of Interest (OCI)

(a) The attention of the Respondent is directed to FAR Subpart 9.5 relating to Organizational Conflicts of Interest (OCIs).

(b) If applicable, prospective Respondents are requested to furnish with their technical papers information regarding any existing or potential conflicts of interest.

(c) It is the responsibility of the Respondent to identify and disclose OCIs. Respondents shall address any existing or potential OCIs in their proposals and shall include a plan to mitigate all OCIs identified. The Government intends to evaluate only the mitigation plan of the apparent successful Respondent (if provided). The mitigation plan will not be part of the technical evaluation. However, the Government may reject proposals from Respondents with OCIs that are not adequately mitigated. The proposed mitigation plan must mitigate all conflicts of interest such that the full scope of work contemplated in this solicitation may be performed by the Respondent. Failure to disclose OCI issues known or identified prior to award or discovered after award, or misrepresenting relevant information to the Contracting Officer, is grounds for termination for default, debarment from Government contracts, and/or other remedies permitted by law or this contract.

(d) An OCI mitigation plan, if submitted, should address but not be limited to the following information:

- How the company plans to identify and track actual or potential OCIs;
- How source selection information or proprietary data will be physically safeguarded (e.g., locked file cabinets, safes, etc...);
- How company personnel working on the contract will be segregated from the rest of the company workforce and, if required, report through separate chains of command;
- Data security measures, including how computer workstations dedicated to the contract will be maintained in separate, secure areas and will require unique passwords for access;
- How the company plans to handle an improper disclosure of sensitive information and how it is communicated to the Contracting Officer;
- How the OCI clause is flowed down to subcontractors and how it is administered;
- Training of personnel in their non-disclosure and procurement integrity responsibilities including penalties the company may impose if sensitive information is disclosed;
- The process for obtaining NDAs executed between the company and subcontractors as well as those signed by company employees.

10.2 Unauthorized Disclosure

Technical papers submitted under this BAA will be protected from unauthorized disclosure in accordance with FAR 3.104-5 and 15.207. Government personnel will perform the evaluation of technical papers. Support contractors, as identified in Section 4.2, may assist for administrative purposes only. Technical paper selection and award decision are solely the responsibility of Government personnel. Any individual having access to technical papers, the SOW, and/or the cost proposal submitted in response to this BAA will be required to sign a NDA prior to receipt of any technical paper submissions.

APPENDIX A: Certification and Accreditation Regulations: Information Assurance Rules and Regulations: Required IA Capabilities Support

- ***Executive Order 12958, Classified National Security Information***, amended 25 March 2003, is applicable because it specifies requirements for safeguarding national security information.
- ***DoD Instruction (DoDI) 5200.40, “DoD Information Technology Security Certification and Accreditation Process (DITSCAP)”***, 30 December 1997, implements policy, assigns responsibilities, and prescribes procedures for Certification and Accreditation (C&A) IS, including automated information systems, networks, and sites in DoD.
- ***DoD 8510.1M, “Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual,”*** 21 July 2000, establishes a standard process, set of activities, general tasks, and a management structure to certify and accredit Information System (IS) that will maintain the Defense Information Infrastructure (DII).
- ***DoD Directive (DoDD) 8500.1, “Information Assurance (IA),”*** October 24, 2002, provides mandatory minimum-security requirements. DoDD 8500.1 establishes policy and assigns responsibilities under title 10, United States Code (U.S.C.), Armed Forces, Section 2224, Defense Information Assurance Program to achieve DoD IA through a defense in depth approach that integrates the capabilities of personnel, operations and technology, and supports the evolution to network centric warfare.
- ***Department of Defense Instruction (DoDI) 8500.2, “Information Assurance (IA) Implementation,”*** 6 February 2003, implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks.
- ***Secretary of the Navy Instruction (SECNAVINST) 5239.3, “Department of the Navy Information Systems Security (INFOSEC) Program,”*** July 14, 1995, establishes DON policy for the INFOSEC Program within the Information Warfare (IW) discipline and to define the organizational responsibilities for implementation of the security disciplines of Communications Security (COMSEC), Computer Security (COMPUSEC), and Emanations Security (TEMPEST).
- ***National Security Telecommunications and Information Systems Security Policy (NSTISSP) No.11, “National Information Assurance Acquisition Policy,”*** January 2000, which states that IA shall be considered as a requirement for all systems used to enter, process, store, display, or transmit national security information.
- ***Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources***, requires that systems provide a level of security commensurate with the sensitivity of the information, the risk of unauthorized access, and the harm that could result from improper access. OMB Circular A-130 requires that a security program be established to safeguard the sensitive information that it processes.
- ***DS-2610-142-01, “Joint DoDIIS/Cryptologic SCI Information Systems Security Standards.”*** The MPRF Expeditionary Capability will be deployed on SCI and GENSER SECRET networks. It is supported by the DoD Intelligence Information Systems (DoDIIS) Security Certification and Accreditation process as described in accordance with DoDIIS Security Guide ***DS-2610-142-01***.
- ***DCID 6/3, Protecting Sensitive Compartmented Information Within Information Systems.”*** Director Central Intelligence Directive ***DCID 6/3*** establishes security criteria, policy and procedures for storing, processing, and communicating classified intelligence information in information systems (IS). In order to ensure accreditation at both the GENSER and SCI levels, the more restrictive set of security

requirements – those specified by Director of Central Intelligence Directive (DCID) 6/3, have been identified for the system design. Based on the criteria defined in, the C2I portion must meet the security requirements of Protection Level 2 with an Integrity and Availability Level of Concern (LOC) of Medium.

- ***DoDI 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),”*** November 2007.
- ***Intelligence Community Directive Number 503,*** Intelligence Community information Technology Systems Security Risk Management, Certification and Accreditation effective 15 September 2008.
- ***Joint Air Force Army Navy JAFAN 6-3,*** Security policy and procedures for storing, processing, and communicating classified DoD Special Access Program (SAP) information in information systems (IS).

APPENDIX B: RELEVANT EXPERIENCE FORM

1. Complete Name of Reference (Government agency, commercial firm, or other organization)	
2. Complete Address of Reference	
3. Contract Number or other control number	4. Date of contract
5. Date work was begun	6. Date work was completed
7. Contract type, initial contract price, estimated cost and fee, or target cost and profit or fee	8. Final amount invoiced or amount invoiced to date
9a. Reference/Technical point of contact (name, title, address, telephone no. and email address)	9b. Reference/Contracting point of contact (name, title, address, telephone no. and email address)
10. Location of work (country, state or province, county, city)	
11. Current status of contract (choose one): <input type="checkbox"/> Work continuing, on schedule <input type="checkbox"/> Work continuing, behind schedule <input type="checkbox"/> Work completed, no further action pending or underway <input type="checkbox"/> Work completed, routine administrative action pending or underway <input type="checkbox"/> Work completed, claims negotiations pending or underway <input type="checkbox"/> Work completed, litigation pending or underway <input type="checkbox"/> Terminated for Convenience <input type="checkbox"/> Terminated for Default <input type="checkbox"/> Other (explain)	
12. Provide brief information describing the success of your firm in furthering the policy of the United States to maximize practicable opportunities for small business concerns, HUBZone small business concerns, small business concerns owned and controlled by socially and economically disadvantaged individuals, and small business concerns owned and controlled by women to participate in this contract.	
13. When contracting with firms described in part 12 above, describe what, if any, procedures your firm established to ensure timely payment of amounts due.	
14a. Did this contract require a Small Business Subcontracting Plan pursuant to FAR 52.219-9? Yes ____, No ____. 14b. If "Yes" to 14a, have you regularly submitted SF 294/295 reports on time? Yes ____, No ____. 14c. Attach a copy of your most recently submitted SF 294.	
15. Provide a summary description of contract work, not to exceed two pages in length. Describe the nature and scope of work, its relevancy to this contract, and a description of any problems encountered and your corrective actions. Attach the explanation to this form.	
16. Indicate if Past Performance information for this contract is located in the Contractor Performance Assessment Reporting System (CPARS), the Past Performance Information Retrieval System (PPIRS) or not in either system.	