**Title Page**

**Contents**

Subfactor One - Subfactor 1: Cybersecurity/Information Assurance 3

*6.5 Task 5 – Cybersecurity (CS) 3*

*6.8 Task 8 – Cyber Threat Security Plan 3*

*(a) Handling of Non-Public Information. (b) Cyber Threat Security Plan. Deliverable: Cyber Threat Security Plan 4*

Subfactor Two - Subfactor 2: Program Management 4

*Management Plan 5*

*6.1 Task 1 – Task Order Management Support 5*

*The on-site task order project manager (PM) is the principal point of contact… 6*

Subfactor Three - Subfactor 3: Command, Control, and Communications Protection (C3P) Ashore Support 6

*6.2 Task 2 – Command, Control, and Communications Protection (C3P) Ashore Support 6*

Subfactor Four - Managed IT Services Support 7

*6.3 Task 3 – Enterprise/Infrastructure Services Support 7*

*6.6 Task 6 – Managed IT Services Support 7*

*6.7 Task 7 – Bilateral Communications and Network Management Support 8*

*6.4 Task 4 – Enterprise Architecture 8*

Staffing Plan 9

*Training 10*

*Surge Support 11*

*Recruiting and Retention 11*

*Security Considerations 11*

Transition 12

Quality Assurance 13

*Approach to Quality 13*

*7. Performance Standards. 13*

**List of Table and Drawings**

**Glossary**

# Subfactor One - Subfactor 1: Cybersecurity/Information Assurance

Subfactor 1: Cybersecurity/Information Assurance — The Contractor demonstrates a plan and process for managing Cybersecurity/Information Assurance workload in compliance with applicable DoD, DoN, and HQ instructions, policies, and procedures such as DoD Instruction 8500.01 (Subtask 6.5.1). The Contractor demonstrates technical proficiency in managing Risk Management Framework (Subtask 6.5.3) The Contractor demonstrates technical proficiency in managing Incident response processes (Subtask 6.5.5).

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## 6.5 Task 5 – Cybersecurity (CS)

The Contractor shall provide CS support for the CNFJ / CNRJ and installation sites. Contractor will implement approved CS standards IAW prescribed NIST, DoD, DoN and CNIC as Information Systems Security Officers (ISSOs) and Appointees with direction from the Regional Information Systems Security Manager (ISSM), assuring the Confidentiality, Integrity, Availability, Non-Repudiation and Accountability are maintained for systems within the command’s area of operation. Applicable governing policy includes, but is not limited to, DoD Instruction 8500.01, SECNAV Instruction 5239.3C, SECNAV M-5510.36 and DoN CIO Cybersecurity Strategy Guidance. Contractors designated in CS roles will maintain separation of duties IAW DoD and DoN guidance.

Subtask 1– CS Program Management

Subtask 2 – System/Access Control Management

6.5.3 Subtask 3 –Assessment and Authorization (A&A)

Subtask 4– Audit and Compliance Management

Subtask 5 – Incident Handling and Response

Subtask 6 – Inspections, Assessments, and Visits

Subtask 7 – PKI and Site Trusted Agent (STA)

Subtask 8 – CS/IA Awareness and Training

Subtask 9 – CS Workforce Management

Subtask 10 – Installation CS Support

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## 6.8 Task 8 – Cyber Threat Security Plan

a) Handling of Non-Public Information

b) Cyber Threat Security Plan

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## (a) Handling of Non-Public Information. (b) Cyber Threat Security Plan. Deliverable: Cyber Threat Security Plan

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

# Subfactor Two - Subfactor 2: Program Management

Subfactor 2: Program Management — Details the plan and process to meet the response times in Table 1: Service Call Response and Completion Time (Task Areas 2, 3 & 5), and Table 2: Service Call Response and Completion Time (Task Areas 6 & 7) of the PWS. Demonstrates a comprehensive management approach that ensures fully- qualified, appropriately certified personnel are provided to meet all requirements of the PWS as specified in Paragraph 13.2.9 Qualifications, including the appropriate mix of labor categories, labor hours, and other direct costs to meet the requirements of the PWS. Contractor's proposal shall include a staffing plan that identifies each position, supplemented with resumes for review.   
Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## Management Plan

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## 6.1 Task 1 – Task Order Management Support

The on-site task order project manager (PM) is the principal point of contact for activities under the task order. The PM will receive technical direction from the COR and then delegate or distribute work assignments as necessary. It is the PM’s responsibility to manage, monitor, and report on all task assignments.

Contractor shall:

a) Provide an on-site centralized and authorized PM as the point of contact with the Government COR. PM responsibilities include, but are not limited to, interfacing with Government management personnel, staffing of all tasks, formulating, and enforcing work standards, creating personnel and project schedules, reviewing work discrepancies, and communicating Government policies, purposes, and goals to the contractor team.

b) Prepare, maintain, and follow a Task Order Management Plan (TOMP) outlining the management approach, management controls, organizational resources to be employed, deliverables and delivery dates. This TOMP shall be provided and agreed upon by the Government within 30 working days of contract award. The contractor shall update the plan each option year within 15 working days of the option exercised.

c) Deliver a finalized Transition-In Plan within 5 working days of award that ensures minimal service disruption to vital Government business and no service degradation during and after the Transition-In period. All transition-in activities shall be completed from 1-31 July 2022.

d) Provide and implement a Transition-Out Plan within 45 working days prior to expiration or notification of contract termination. To ensure a seamless transition, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

Project management processes

Points of contact

Location of technical and project management documentation

Schedules and milestones

Status of ongoing technical initiatives

Appropriate contractor-to-contractor coordination

Transition of key personnel

Actions required of the Government

File plan, work related documents, files, policies and processes

Inventories of hardware (H/W) and software (S/W)

Access permission by individuals to locations in which they support   
e) Provide Employee Assignment Notification of employee replacements and reassignments no later than 5 days after the contractor is notified or has taken action, whichever is earlier. Notification shall include a transition plan and expected date of staffing.  
Deliverables: Task Order Management Plan (TOMP)   
Transition-In Plan Transition-Out Plan

6.1.1 Subtask 1 – Program Kick-off Meeting

6.1.2 Subtask 4 – Contractor’s Progress, Status and Management Report   
Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## The on-site task order project manager (PM) is the principal point of contact…

# Subfactor Three - Subfactor 3: Command, Control, and Communications Protection (C3P) Ashore Support

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## 6.2 Task 2 – Command, Control, and Communications Protection (C3P) Ashore Support

The Contractor shall perform a variety of complex assignments associated with managing, maintaining, and controlling Regional Operation Center (ROC), Emergency Operations Centers (EOCs) Regional Dispatch Center (RDC) and Local Dispatch Center (LDC) IT and communications systems. Applicable governing policy includes, but is not limited to, CNIC Instruction 5222.1 para 4.j. and 5.g.

Subtask 1– ROC/EOC/RDC/LDC Support

Subtask 2 – Emergency Communications Support

Subtask 3 – Entry Control Point (ECP)/Access Control Systems (ACS) Support

Subtask 4 – Public Safety Network (PSNet)/Anti-Terrorism Force Protection (ATFP) Support

Subtask 5 – Enterprise Land Mobile Radio (ELMR) Support

Subtask 6 – RDC Alarms Manager

Assigned to: \_\_\_\_\_\_\_\_\_

* 1. Task 2 – Command, Control, and Communications Protection (C3P) Ashore Support.

A significant challenge to the Navy Program is the successful implementation of IT services that respond to the evolving needs of the warfighter at a broad range of dispatch and operations centers meeting C3P requirements. These services must be integrated to provide an end-to-end solution that performs to the C3P service levels (or better) and strive to reduce costs throughout the life of the program and individual tasks. [TEAM] has the capabilities to meet these challenges and has demonstrated experience supporting various C3P systems for multiple agencies.

* + 1. Subtask 1– ROC/EOC/RDC/LDC Support.

Support of Operations and Dispatch Centers must address not only the technological but the operational needs of the warfighters and provide seamless operations of these critical centers. [TEAM] uses proven methodologies, standards and practices from Information Technology Information Library (ITIL) and Help Desk Institute (HDI) to provide technical support functions. Application of ITIL and HDI frameworks and processes allow us to define, implement, monitor, and refine our level of service provide a program of continual service improvement. Furthermore, use of standard practices provides continuity of operations in the event of emergencies, staff changes, or system rollouts. Our System Administration functions will coordinate with various other sustainment providers to ensure that hardware and software deployed in each dispatch and operation center is properly maintained, up-to-date and mission-ready.

* + 1. Subtask 2 – Emergency Communications Support.

[TEAM] currently provides Enhanced Mobile Satellite Service (EMSS) devices and service to government users enabling satellite communications and location. We provide full support to provide and configure devices and provide ongoing service and support for users. We have access to Broadband Global Area Network (BGAN) systems as well also providing hardware and services as through our other contract vehicles. We support our deployed field staff with reach back support when additional resources are needed for technical support issues, logistics or OEM support.

* + 1. Subtask 3 – Entry Control Point (ECP)/Access Control Systems (ACS) Support.

[TEAM] staff will provide technical support and training for Defense Biometric ID System (DBIDS) elements deployed at installations throughout the region. We will coordinate with local commands to establish needed training sessions and schedules and provide troubleshooting and technical support for deployed systems as needed. When upgrades and replacement of equipment is required, our staff will coordinate installations, communicate any operational impacts to affected groups and enterprise level staff, receive and inventory equipment, manage installations, documentation and ongoing operations as needed. Other ECP/ACS systems other than DBIDS will be managed as needed according to policy.

* + 1. Subtask 4 – Public Safety Network (PSNet)/Anti-Terrorism Force Protection (ATFP) Support.

[TEAM] recognizes that the most critical factor in maintaining peak efficiency and availability to any mission critical service is proactive system support activities such as network maintenance, network planning, and systems monitoring. [TEAM] has extensive experience in performing O&M activities for other enterprise services and their components to include NIPRNet and SIPRNet (both CONUS and OCONUS). We will provide ongoing support for the deployment of new systems connected through PSNet and will coordinate with the appropriate ATFP sustainment organization as equipment is installed and/or decommissioned and deliver the ATFP IT Systems Report quarterly detailing any completed or pending changes to systems over the previous quarter.

* + 1. Subtask 5 – Enterprise Land Mobile Radio (ELMR) Support.

The ELMR system provides instant communication and interoperability between users both at a base level but also between various installations across commands. [TEAM] has over two decades of experience in designing, deployment and maintaining ELMR system infrastructure and subscribers with established relationships with major OEMs including Motorola Solutions and Harris. We have provided support for ELMR Project 25 (P25) system core installation and upgrades, new RF site design and maintenance. Our deployed team will have access to our team of LMR engineers to support advanced fleetmapping and programming techniques. We provide training on a variety of topics including RF principles and subscriber operations. Our engineering teams can provide guidance with ongoing system lifecycle and upgrade plans to ensure that when various components require upgrades, plans are developed to ensure that systems are always fully supportable and mission capable.

* + 1. Subtask 6 – RDC Alarms Manager.

Local base fire and instruction alarms will be managed as part of each Local and Regional Alarm Management systems by ensuring proper administration and testing of each system including integration with Computer Aided Dispatch (CAD) at each site. Each alarm node will require support of the various connectivity methods whether twisted pair or radio connectivity, which will be managed by our deployed team as a function of other subtasks. Server and Database management will be performed both at the local and regional levels to ensure proper updates for configuration changes as systems are repaired or upgraded. Proper integration between the RAMAS/LAMAS and local CAD and GIS systems will be regularly tested to ensure proper operation with temporary monitoring and reporting mechanisms enabled in the event of a failure of the CAD interface with an alarm server.

# Subfactor Four - Managed IT Services Support

a. The Contractor demonstrates a plan for effectively managing C3P workload under the following tasks in compliance with applicable DoD, DoN, and HQ instructions, policies, and procedures such as CNIC Instruction 5222.1 para 4.j and 5.g. PWS Subtask 6.2.1 - ROC/EOC/RDC/LDC Support. PWS Subtask 6.2.2 - Emergency Communications Support. PWS Subtask 6.2.3 - Entry Control Point (ECP)/Access Control Systems (ACS) Support. PWS Subtask 6.2.4 - Public Safety Network (PSNet)/Anti-Terrorism Force Protection (ATFP) Support. PWS Subtask 6.2.6 - RDC Alarms Manager,

Assigned to: \_\_\_\_\_\_\_\_\_

## 6.3 Task 3 – Enterprise/Infrastructure Services Support

The Contractor shall provide support for hosting and technology products mapped to organizational business processes supporting CNIC and Regional mission objectives and decision making. Technology products and processes provide data analytics and tools to CNIC N-codes through dashboard visualizations, data warehousing, collaboration, and technology infrastructure and network services. The Contractor shall stay abreast of the latest technology to support CNIC SharePoint services, Systems Administration, Microsoft Office Suite products (Office 365, Microsoft Teams and CVR), Cloud solution and new IT solutions that become available and required to support the CNIC mission.

Subtask 1 – Platform Application Management

Subtask 2 – Application Strategy Management

Subtask 3 – Operational Application Management

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## 6.6 Task 6 – Managed IT Services Support

As part of the Region or Installation IT staff, the Contractor shall provide support based on Information Technology Infrastructure Library (ITIL) framework of IT services to internal departments with application and systems support to include web, database, and other specialized applications or programs; support to other Departments in the migration or implementation of CNIC enterprise IT initiatives, web or portal sites and application software.

Subtask 1– CNIC and ONE-NET Liaison support

Subtask 2 – Systems and Network Support

Subtask 3 – Video Teleconference Support

Subtask 4 – Asset Management Support

Subtask 5 – Telephone Control Officer (TCO) Support

Subtask 6 – Life Cycle Management. 6.6.6.1 The Contractor shall document their findings for all BOM requests… 6.6.6.2. The Contractor is responsible for proper receipt, handling, storage, and accountability of items ordered

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## 6.7 Task 7 – Bilateral Communications and Network Management Support

The Contractor shall provide Regional oversight and business management of Bilateral-Telecommunication and Networks infrastructure including assisting in the requirements development, implementation, operation and maintenance of technologies or capabilities as directed by Echelon II Mission Stakeholders.

Subtask 1– Bilateral Communications Analysis and Support

Subtask 2 – Bilateral Program Coordination

Subtask 3 – Bilateral System Support (i.e., CENTRIXS, ADSI, GCCS, and RADMERC)

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## 6.4 Task 4 – Enterprise Architecture

The Contractor shall provide portfolio management knowledge management, portal contents development and implementation support for CNRJ / CNFJ and its installation sites in accordance with guidance provided by CNIC and higher authority. The Contractor shall assist CNRJ / CNFJ with identifying those functions and capabilities required in order to ensure they are best satisfied and preserved within the Region Japan IT portfolio. CNRJ / CNFJ is responsible for the on-going management of the IT Portfolio processes and tasks as the Region Japan Portfolio lead. These processes and tasks are in place to continue streamlining IT overhead within the DOD. The reduction and consolidation of the duplicative IT systems, applications, and databases through the guidance of the CNIC and higher authorities. The Contractor shall also conduct research on technology trends and documentation as required.

Subtask 1 – DADMS / DITPR-DON database record update   
Subtask 2 – Portfolio Customer Support

Subtask 3 – Portfolio Management Liaison Support

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

# Staffing Plan

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

Top Secret security clearance and final IT-I (privileged level systems access), and immediately upon hire, will also require SCI access eligibility:

Bilateral Communications and Network Management Support

The following types of positions require a minimum interim Secret security clearance and interim IT-II eligibility when performance starts:

Program Management  
C3P Ashore Support  
Enterprise / Infrastructure Services Support

Enterprise Architecture  
Cybersecurity / Information Assurance

Installation Cybersecurity Support  
Managed IT Services Support  
Bilateral Communications Analysis and Support

Roles:

Program Management. Minimum of ten years of experience in environments similar to that of the contract and:

Demonstrated experience managing and supervising employees in labor categories and with skills applicable to programs similar in size and scope.   
Demonstrated experience with the DoD acquisition process.   
Demonstrated knowledge of Navy financial management processes.

C3P Ashore Support. Minimum of five years of experience in a related IT field and:   
Technical knowledge of the ROC / EOC / RDC / LDC operational and hardware design infrastructure.

Thorough knowledge of maintenance of trunking mobile, base stations and handheld subscriber units   
and antennas.

Technical knowledge of PSNet architecture and the systems utilizing PSNet.

Thorough knowledge of ATFP systems under the ATFP global sustainment contract.

Technical knowledge of applicable DoD, DoN, and HQ instructions, policies, and procedures.

Meets CSWF qualifications required for Specialty Area 451 – System Administration (Journeyman).

Enterprise/Infrastructure Services Support. Minimum of two years of experience in a related IT field and:

Demonstrated experience in SharePoint 2013.

 Excellent customer service/support skills.

Demonstrated experience in System Administration.

Meets CSWF qualifications required for Specialty Area 451 – System Administration (Journeyman) and   
Operating System Certification (Minimum requirement MS Server 2016 cert or Azure 104+500 certs).

Enterprise Architecture. Minimum of three years of experience in a related IT field and:

Excellent customer service/support skills.

Strong communications skills to interface with Portfolio Management related counterparts to include   
higher echelon staff, other Navy organizations and vendors.

Ability to track and maintain the requests which can exceed multiple years.

Technical knowledge of applicable DoD, DoN, and HQ instructions, policies, and procedures.

Meets CSWF qualifications required for Specialty Area 804 – Portfolio Manager (Journeyman).

Cybersecurity/Information Assurance (Section 6.5.1-6.5.9). Minimum of five years of experience in a related IT field and:

Knowledge of applicable DoD, DoN, RMF and HQ instructions, policies, and procedures.

Meets CSWF qualifications required for Specialty Area 461 –Systems Security Analyst (Intermediate) or Specialty Area 541 Vulnerability Assessment Analyst (Intermediate)

Installation Cybersecurity Support (Section 6.5.10). Minimum of three years of experience in a related IT field and: Knowledge of applicable DoD, DoN, RMF and HQ instructions, policies, and procedures.

Meets CSWF qualifications required for Specialty Area 461 – Systems Security Analyst (Intermediate) or Specialty Area 541 Vulnerability Assessment Analyst (Intermediate)

Managed IT Services Support. Minimum of three years of experience in a related IT field and:

Technical knowledge of Navy ONE-Net (OCONUS Enterprise Network) processes and procedures, to include applicable CNFJ / CNRJ procedures, applicable Request for Change form (RFC) procedures, help- desk tickets and Move-Add- Change (MAC) procedures as applied withinCNFJ.

Technical knowledge of applicable DoD, DoN, and HQ instructions, policies, and procedures.

Meets CSWF qualifications required for Specialty Area 411 – Technical Support Specialist (Journeyman)

Bilateral Communications Analysis and Support. Minimum of three years of experience in a related IT field and:

Demonstrated experience in bilateral communications analysis and support, to include significant knowledge of governing processes and policies.

Strong communications skills to interface with DoN/DoD staff, managers, and foreign military counterparts.

Ability to independently operate amongst and in partnership with host nation military personnel to facilitate execution of the Navy's mission in Japan.

Knowledge of applicable DoD, DoN, and HQ instructions, policies, and procedures.

Meets CSWF qualifications required for Specialty Area 641 – Systems Requirements Planning   
(Journeyman).

Bilateral Communications and Network Management Support. Minimum of three years of experience in a related IT field and:

Technical knowledge of bilateral systems and network architecture.

Demonstrated experience in bilateral communications and network management, to include significant knowledge of governing processes and policies.

Knowledge of applicable DoD, DoN, and HQ instructions, policies, and procedures.  
Meets CSWF qualifications required for Specialty Area 441 – Network Operations Specialist

## Training

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## Surge Support

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## Recruiting and Retention

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## Security Considerations

Assigned to: \_\_\_\_\_\_\_\_\_

11.2 Security Clearance and Information Technology (IT) Level

11.6 Information Security and Other Miscellaneous Requirements - page 183

[Start writing here…]

Other Pertinent Information or Special Considerations

See page 184 ADDENDUM TO 52.212-1 Addendum to 52.212-1(b), Submission of Offers is tailored as follows: (b) Submission of offers: (12) Other Instructions. (page 189 thru 199)

[Start writing here…]

**OCCI Mitigation Plan**

…or a statement that OCCI does not exist, per (iii) IAW DISA Special Contract Requirement H1, each offeror shall specifically identify in its proposal whether or not any potential or actual Organizational and Consultant Conflicts of Interest (OCCI), as described in Federal Acquisition Regulation (FAR) Subpart 9.5, exists for this instant procurement. If the offeror believes that no OCCI exists, the OCCI response shall set forth sufficient details to support such a position. If an offeror believes that an actual or perceived OCCI does exist on the instant procurement, the offeror shall submit an OCCI plan with the proposal, explaining in detail how the OCCI will be mitigated and/or avoided.

[Start writing here…]

# Transition

13.4 Transition/Mobilization/De-Mobilization. The Government will not provide any funds for the transition, mobilization and de-mobilization of the Contractor employees, household goods, or family members.

13.5 Transition-In Period. The phase-in period encompasses the people, processes, tools, technologies, and sequenced activities required to transfer service operations from the incumbent Contractor. The phase-in period is projected to be approximately 30 days.

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

# Quality Assurance

Assigned to: \_\_\_\_\_\_\_\_\_

[Start writing here…]

## Approach to Quality

## 7. Performance Standards.

7.1 Service Calls. 7.1.1 Response Times. 7.1.2 Cell Phone Availability. 7.1.3 Completion Time Delays. 7.2 Acceptable Quality Level. See page 177 of RFP PWS

Address the Quality Assurance Surveillance Plan (QASP) referencing a draft QAP