**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: \_\_\_\_\_\_\_\_\_

# 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:ActioNet

Our processes are compliant with:

* CMMI Level 4 (Services and Development)
* ISO 9001 (Quality)
* ISO 20000 (ITIL)
* ISO 27001 (Cyber Security).

Team AveningTech draws on our vast experience and expertise operating large­scale IT Support and Service Desk operations for our federal customers and determining most efficient and optimum staffing levels. Our approach will deliver several key elements:

* Smooth seamless transition with no disruption to the mission
* Effective and efficient knowledge transfer
* Established Service Desk ITIL­based, ISO­certified processes and procedures that comply with Help Desk Institute (HDI) best practices
* A proactive approach that will meet and consistently exceed SLA
* Constant SLA monitoring and establishing proactive remediation before the threshold is reached
* Initial and periodic refresher training and monitoring for any chronic staff issues that would trigger an upgrade of staff
* Service Desk operators applying innovation directly into the tool without going through a third party/contract
* Cost efficiency through innovation, automation, and efficiency.

Infrastructure Solutions for enterprise infrastructure improvement, platform migrations, network

engineering and administration, server hardware and software operations and management,

email systems and Help Desk support. Team AveningTech is adept at applying ITIL best practices and

exploiting technologies to improve service delivery and availability with reduced labor costs.

Team AveningTech provided 24x7x365 enterprise level support of Navy Enterprise Data Center (NEDC) infrastructure (classified and unclassified enclaves) and cloud hosting services to include Windows, Unix, Linux, Network, Network Security, Storage, Domain Name Services (DNS), Backups, Databases, Virtualization including Hypervisor and Application, Host Based Security Systems (HBSS), Assured Compliance Assessment Solution (ACAS), and Cloud Hosting services. Collectively our system administrators and engineers installed, configured, and maintained Solaris, RedHat, and Microsoft Windows operating systems supporting 1,550+ servers (Windows 1025, Linux 410, Solaris 140) and over 500,000 user accounts in support of both classified and unclassified domains. Additionally, ActioNet has provided remote support to NIWC Charleston and Kansas City datacenters to include over 1,800+ servers (Windows 1300, Linux 360, Solaris 150). Our Cybersecurity Workforce (CSWF) staff are experts at implementing Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), maintaining tight patching standards, and integrating those into baseline requirement standards. Team AveningTech directly supported the DC2HS Navy Cloud Broker (NCB) team and provided technical support for the migration of 53 systems from NIWC LANT NEDC-hosted environments to IL2 and IL4 certified Amazon We Services (AWS) and Azure environments. This migration resulted in the creation of 600+ virtual server instances across GovCloud and Public cloud regions (test and development environments).

6.3.1 Subtask 1 - Platform and Application Management

Team AveningTech will provide SharePoint Administration support ensuring a well-maintained and well

performing CNFJ / CNRJ Gateway and ONE-Net SharePoint portal. Our staff will monitor the day-to-day performance of the workflows ensuring they are active. We will correct any problems with workflows and applications and maintain the organization changes as needed.

Team AveningTech will administer, maintain, and monitor the CNFJ/CNRJ SharePoint sites host in Microsoft 365 environment. We will bring the following significant factors to support the SharePoint environment:

* Design and implement automated reports to eliminate manual processing and streamline document gathering/tracking across the agency
* Provide project templates, status reporting forms and reporting dashboards according to best-practice processes
* Build an accessible SharePoint Site and Fix any SharePoint sites which are not compliant
* Consult with internal leadership and stakeholders to determine needs and develop SharePoint solutions
* Upload, organize, and maintain SharePoint program and project documentation, calendars, meeting information, and other workspaces
* Train new users on basic functional use of SharePoint
* Update and reorganize the information on the existing SharePoint system
* Review the SharePoint system and propose basic and custom modifications to improve the system’s functionality, effectiveness, and efficiencies.
* Maintain SharePoint Sites, SharePoint Lists Features, Custom Workflows, Nintex Workflows and Document Libraries
* Our quality and service management framework that is founded upon internationally recognized
* and independently certified ISO 9000, 20000, and 27000 processes.

Team AveningTech uses a comprehensive approach to perform all SharePoint administrative activities that ensures day-to-day operations run smoothly. Leveraging our experience at the US Courts, our team will develop a SharePoint Governance Plan (SGP) SGP that includes a detailed analysis of all workflows and CNF/CNRJ sites that require maintenance. Our SGP establishes quantified goals and measures for system operations to ensure a well-maintained and well-performing portal. The SGP governs site configuration and maintenance activities across the tenant, hub, and local levels ensuring support standardization across the instance. All authorized changes to the system will be supported as well as any issue including creating sub sites, managing permissions, creating pages, customizing the web parts, and. creating workflows. External and internal access is audited and reported regularly to ensure data integrity as well as confirm compliance with the permissions matrix and the SGP. We monitor Microsoft 365 service health, workflow and webpart error alerts, as well as storage and usage statistics in the “Admin Center” to confirm the health of the system and avoid content overloading. All planned and unplanned work performed will be tracked within appropriate stories and tasks. The SGP establishes a set schedule for all operations and maintenance activities and deliverable dates as desired by CNFJ/CNRJ stakeholders. Utilizing the Agile methodology, we can create a site to track the status of new projects and change management requests received from the SharePoint mailbox. We incorporate quality controls into the SharePoint Governance Plan (SGP) to confirm every phase of the project is completed and documented as per set standards.

6.3.2 Subtask 2 - Application Strategy Management

Team AveningTech will leverage our Navy Enterprise Asset Management experience maintaining compliance and utilization of Navy enterprise toolsets, development frameworks, and networks such as Navy/Marine Corps Intranet (NMCI), NMCI Enterprise Tool (NET), and DON Application and Database Management System (DADMS) to ensure enterprise architecture and interoperability across all CNFJ/CNRJ systems.

For the Naval Information Warfare (NIWC) Atlantic Data Center and Cloud Hosting Services (DC2HS) Operations Center and Sustainment contract, Team AveningTech provided application management services in addition to other data center operations and maintenance requirements. Other services included IT planning, analysis, evaluation, testing, security, documentation, logistics, administration, monitoring, alerting, and operational sustainment support required to accomplish specified tasks. The DC2HS Division is tasked with providing a hosting environment for Navy applications and other Department of Defense (DoD) and Homeland Security (HLS) applications utilizing both Component Enterprise Data Centers (CEDC)s and Commercial Service Providers (CSP)s as hosting platforms. DC2HS hosting services reside on various networks including the Extended Demilitarized Zone (eDMZ) provided by NGEN, NIPRNET and SIPRNET provided by DISA, SIPRNET, and commercial internet providers hosting CSPs. Within each hosting platform, DC2HS provides a set of common services as Shared Services to resident mission owners.

Team AveningTech performed system software updates, tuning, patching, administration, monitoring, maintenance, IAVM patching, DADMS registration, STIG implementation, maintaining security compliance, CTO responses, auditing and logging, and reporting. We also supported the ability to Interpret server operational characteristics, accurately determine the presence of a problem, and identify possible solutions for the below and ensure configurations are in line with industry best practices. We provided enterprise-wide management and engineering support of system backups and worked closely customers to overcome challenges (i.e. data integrity) to ensure hosted data/systems were backed up and restored as required.

Team AveningTech implemented a robust, streamlined configuration management process to ensure all assets, software, and documentation were managed according to the baseline and stored in the NIWC LANT configuration repository – Dimensions CM. We worked closely with technical service managers (TSMs), using NMCI Enterprise Tool (NET) to manage enterprise assets, service catalogs, and change service requests. The benefit to the customer was a streamlined workflow process that resulted in enterprise-wide asset management and configuration control of DON approved software. All utilized hardware/software maintained 100% compliance with Department of the Navy Applications and Database Management System (DADMS).

3.3 Subtask 3 - Operational Application Management

Team AveningTech’ s cross-cutting performance approach focuses on utilizing Scaled Agile Framework (SAFe) using the DevSecOps process which will automate the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and delivery. DevSecOps within a cloud environment allows for quick and easy deployment strategy with multiple environments to include Ashore and Afloat. Our services include Application Maintenance and Sustainment, Application Management, Application Hosting, Application Help Desk, and Application Training. This support will provide all the services necessary to establish and manage the CNFJ/CNRJ business application portfolio. Team AveningTech will leverage our experience in operational application management that will result in the following benefits to the CNFJ/CNRJ applications portfolio:

a. Accelerated solution delivery: Identify and implement innovative industry standards and rapid models for delivering application maintenance and sustainment solutions

b. Improved customer responsiveness: Provide metrics demonstrating and tracking on- demand response times and associated skill sets to address time sensitive categories of application advancement and management requirements

c. On-time solution delivery: Reduce tasks and project schedule delays and the need to rebase-line task and project schedules through improved scheduling, resource availability, industry standards, and utilizing PMP and CMMI best practices

e. Merge the Software Development Life Cycle (SDLC) with the Systems Engineering Framework (SEF): Establish, implement, and incorporate SDLC processes within the SEF to enhance task and project management and business operating model symmetry with other IMCOM and the selected hosting environment.

f. Improved communication skills: Identify and implement methodologies and processes to keep customers and other stakeholders aware of individual application task and project progress. Establish robust communication channels to collect customer feedback, adjust for improvement, and deliver improved services.

g. Incorporation of industry best business practices: Demonstrate continued adherence to Capability Maturity Model Integration (CMMI) - Development Level 4 processes.

For NIWC LANT, we worked closely with technical service managers (TSMs), using NMCI Enterprise Tool (NET) to manage enterprise assets, service catalogs, and change service requests. The benefit to the customer was a streamlined workflow process that resulted in enterprise-wide asset management and configuration control of DON approved software. All utilized hardware/software maintained 100% compliance with DADMS.

## 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 – not evaluated

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: \_\_\_\_\_\_\_\_\_

Team AveningTech will provide regional oversight and business management of all Bilateral-Telecommunications and Network infrastructure including assisting in the requirements development, implementation, operation and maintenance of technologies and capabilities as directed by authorized stakeholders. We will coordinate with USFJ to ensure Bilateral equipment is compatible and will be fully interoperable in the Bilateral operating space. Team AveningTech will assign Network and System Engineers to support the Navy's telecommunications efforts. Leveraging Telecommunication Certification Office Support System (TCOSS), and DISA’s Worldwide On-Line System (WWOLS) these personnel conduct technical studies and design systems on the CNFJ-CNRJ network. We will leverage our experience supporting CENTRIXS-J (Japan-Bilateral Joint Network)​ and CENTRIXS-KOR (Korea-Bilateral Joint Network)​ on our PACAF SIPRNet contract.

6.7.1 Subtask 1 - Bilateral Communications and Analysis Support

Team AveningTech will provide all bilateral program technical analysis in support of bilateral exercises and operations with the Japanese Maritime Self Defense Force (JMSDF). Team AveningTech’ s system administration support will follow its proven technical approach, Continuous Service Improvement Model, to successfully manage systems for scalability, secure administration, and flexibility. We focus on **continuous improvement** based on customer feedback, comprehensive reporting, situational analysis where we regularly assess strengths and weaknesses of a customer’s environment, and lessons learned from other program experiences. We will conduct functional area baseline assessments of processes, data, and operations that measure bilateral communications (telecommunications and networking) operational effectiveness. Through this analysis, we will make recommendations for new hardware, software and processes to improve performance and efficiencies. We will embed Cybersecurity policy from the start, making sure any changes comply with DoD/DON security policies prior to implementation.

6.7.2 - Subtask 2 - Bilateral Program Coordination

Team AveningTech will support CNFJ/CNRJ’s goals by providing support for cross-functional program coordination, issue and risk identification. We will provide advice to, and hands-on support for, project managers in the use of standardized project management processes, tools, and methodologies, facilitate “Lessons Learned” sessions for programs and provide repository for storing related documentation. Team AveningTech’ s onsite project lead will be the single point of contact for all communication security (COMSEC) service-related issues. Team AveningTech will coordinate with USFJ for any Combined Enterprise Regional Information Exchange System - Japan (CENTRIXS-J) related changes in service and keep the command informed on Bilateral telecommunications/network related issues.

6.7.3 Bilateral System Support

Our Systems Engineers will ensure that tactical C4I systems required operational capabilities (ROC’s) reflect interoperability requirements by:

• Assuring that developed tactical C4I systems meet required capabilities by providing day-today system administration, user account administration and system security authorization support

• Perform configuration testing of the C4I systems: GCCS, CENTRXS-J, ADSI, and the Radiant Mercury (RADMERC) Cross Domain Solution (CDS)

• Participate in configuration management of C4I systems from the operational perspective, i.e., additional capability requirements, procedural changes, etc

• Develop and implement interoperability testing procedures, and conduct interoperability testing of tactical C4I systems

• Ensure protocol standards are met - the procedural rules that allow tactical C4I systems to exchange information.

Our candidate for this position has a well-rounded skill set in Network Administration, Centrix-J/K/CNFC, GCCS and honed talents in Cisco networking products. Additionally, he has installed, configured, and maintained Air Defense Systems Integrator (ADSI) for Commander Seventh Fleet onboard the flagship USS Blue Ridge.

## 6.4 Task 4 – Enterprise Architecture – not evaluated

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: \_\_\_\_\_\_\_\_\_

Team AveningTech provides infrastructure architecture support for the US Government (USG)USG including research, design, implementation, and updating of DoD Architectural Framework (DODAF) views in accordance with the latest version, v2.02. We create enterprise architecture views in the customer’s preferred tool with supporting artifacts such as total cost of ownership, roadmap, system, operational, services, standard and data/information viewpoints. The sets of architectures are catalogued to develop sets of Dashboards and Reference Models. Examples of Reference Models Maintain compliance and utilization of Navy enterprise toolsets, development frameworks, and networks such as Navy/Marine Corps Intranet (NMCI), NMCI Enterprise Tool (NET), and DON Application and Database Management System (DADMS) to ensure enterprise architecture and interoperability across all CNFJ-CNRJ systems.

Team AveningTech approach to IT Life Cycle is based on industry best practices such as Project Management Body of Knowledge (PMBOK), CMMI Level 4 DEV and SVC, ITIL, and ISO 9001, ISO 27001, ISO 20000 ITSM frameworks.

Team AveningTech has an in-depth understanding of and experience developing network topology diagrams including but not limited to, the importance of determining network performance, scalability, and proactive reporting and maintenance within the physical and logical aspects. The visual representation of the network’s devices, connections, and paths should be fully represented in topology diagrams to ensure accurate data movement and boundary restrictions have been adhered to, while meeting the applicable security requirements. As it relates to network asset discovery, tools such as SPLUNK are utilized to detect active and inactive assets within the network, in addition to asset communication relationships, and usage within the network. Such discovery tools will provide diagnosis and system outages, device management, configuration management, and identify security risk.

Team AveningTech ensures any equipment/system installed or integrated into Navy platform meets the cybersecurity requirements as specified under DODI 8500.01. We verify that any design change, integration change, configuration change, or installation of hardware and software is in accordance with established DoD/DON/Navy cyber directives and does not violate the terms and conditions of the accreditation/authorization issued by the appropriate Accreditation/ Authorization official.

Subtask 1 - DADMS/DITPT-DON

Team AveningTech’ s robust configuration management approach implements an enterprise toolset solution for configuration identification, status accounting, change control, documentation, and code management/tracking from design through acceptance. Additionally, our CM strategy includes issue management through testing and operations. With more than 15 years of Navy IT experience, we leverage Navy Enterprise Asset Management Tools such as NET and Integrated Solution Framework (ISF)-Tools, as well as ensure compliance with DON Database Management Systems (DADMS) and EAF requirements.

6.4.1 Subtask 2 - Portfolio Customer Support

6.4.2 Subtask 3 - Portfolio Management Liason Support

For the Department of Energy (DoE) OCIO ITSS contract, Team AveningTech served as the trusted integrator, but also as the strategic advisor for the OCIO, including the Chief Technology Officer, Chief Data Officer, Chief Information Security Officer and Chief Architect, and we led the Innovation and Engineering organization to identify opportunities for IT Modernization.

# 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