**VOLUME II - TECHNICAL/MANAGEMENT**

**DRAFT - Version 0.85 6-April-2022**

**Submitted by:**

Avening Management and Technical Services, LLC (AveningTech™)  
11 North Maple Avenue, Suite 101  
La Plata, Maryland 20646  
Tel: 301-848-2053

DUNS: 963340752

**Restrictions on Disclosure of Data**: This proposal includes data that will not be disclosed outside the Government and will not be duplicated, used, or disclosed -- in whole or in part -- for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of -- or in connection with -- the submission of this data, the Government will have the right to duplicate, use or disclose the data to the extent provided in the resulting order. This restriction does not limit the Government’s right to use information contained in this data if it is obtained from another source without restriction.

**Contents**

Subfactor One - Cybersecurity/Information Assurance 1

6.5 Task 5 – Cybersecurity (CS) 2

6.8 Task 8 – Cyber Threat Security Plan 7

Subfactor Two - Program Management 7

6.1 Task 1 – Task Order Management Support 9

Subfactor Three - Command, Control, and Communications Protection (C3P) Ashore Support 11

6.2 Task 2 – Command, Control, and Communications Protection (C3P) Ashore Support 11

Subfactor Four - Managed IT Services Support 13

6.3 Task 3 – Enterprise/Infrastructure Services Support 13

6.4 Task 4 – Enterprise Architecture 17

6.6 Task 6 – Managed IT Services Support 19

6.7 Task 7 – Bilateral Communications and Network Management Support 23

Staffing Plan 24

Transition 29

# Subfactor One - Cybersecurity/Information Assurance

The AveningTech Team will leverage its history of successful cybersecurity support in similar environments. Most notably, we held a prime contract with the US Coast Guard (USCG) Telecommunications and Information Systems Command (TISCOM) to provide cybersecurity subject matter expertise (SME) to TISCOM and USCG’s Field Services Division (FSD). We were responsible for computer network defense (CND) of TISCOM’s networks and computer systems.

In addition to our TISCOM CYBER SME prime contract, we are responsible for cybersecurity activities in support of the US Navy’s Next Generation Enterprise Network (NGEN) on our Service Management, Integration, and Transport (SMIT) contract. AveningTech provides Boundary and Demilitarized Zone (DMZ) Services to protect the NGEN Enterprise, including the management and operation of the boundaries. This support includes support for Cyber Readiness Implementation Plans. We remediate vulnerabilities and misconfigurations, logs and information feeds including HBSS, IPS, and IDS to the MCNOSC. We conduct system-based intrusion detection monitoring and prevention on managed systems and all devices that support HBSS. On the SMIT effort, our cyber security specialists operate all aspects of Information Systems (IS) data availability, integrity, authentication, confidentiality, and non-repudiation. They implement and monitor security measures for communication systems, networks, and provide advice that systems and personnel adhere to established security standards and Governmental requirements for security on these systems. They develop and execute Government approved security policies, plans, and procedures; implement data network security measures; operate and monitor network intrusion detection and forensic systems; conduct IS security incident handling; support Continuity of Operations Plan/Disaster Recovery (COOP/DR) plans, and perform certification of IS and networks. We perform other information security duties including operation of Electronic Key Management System (EKMS) and maintenance of Public Key Infrastructure (PKI). We operate Host Based Security Systems (HBSS), firewalls, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), other point of presence security tools, Virtual Private Networks (VPNs), and related security operations. We perform defensive cyber operation duties including, but not limited to, ensuring workstation and server compliancy with Marine Corps McAfee Host Based Security System (HBSS) requirements; identifying cybersecurity incidents using HBSS, Tenable SecurityCenter, RedSeal, McAfee Security Information and Event Manager (SIEM), and other automated tools; operating Imperva Web Application and Database firewalls; performing forensics and remedial action on cybersecurity incidents; and reporting defensive cyber operations statistics.

Our support includes Malware Detection and Protection Services which provide network-based and host-based malware (malicious code) prevention capabilities with centralized management and reporting. We operate anti-malware software and conduct incident response activity.

We provide Security Event Management (SEM) Services to monitor and correlate security events that are generated from identified networked devices such as firewalls, IPS, and server logs using Government approved filtering strategies and implementations. We monitor and analyze logs and identify unauthorized, illicit, and unwanted activity while providing recommendations to mitigate or respond to threats and vulnerabilities. We maintain CND tools, access control, HBSS, and control modules while operating and defending the network in accordance with all current guidelines. We develop and execute an overall cyber readiness implementation plan. We defend systems by recognizing and responding to threats, identifying and responding to RAs, and analyzing vulnerability scans.

In support of TISCOM we provided technical, operational, administrative, and security management services in the area of cybersecurity on classified and unclassified networks, including the Non-Classified Internet Protocol Router Network (NIPRNET), the Secret Internet Protocol Router Network (SIPRNET), the Department of Defense Information Network (DODIN), and the USCG portion of the Joint Worldwide Intelligence Communications System (JWICS) network.

Our TISCOM support was nearly identical in size and scope to the cybersecurity requirements for this CNFJ/CNRJ effort. We led a team of up to 20 personnel made up of AveningTech employees and subcontractor employees. Our team worked onsite daily with TISCOM and was supported by a dedicated project manager who acted as the interface and liaison between government and contractor personnel.

AveningTech has demonstrated experience and expertise in Information Assurance and understands DoD policies to meet customer IA requirements. We understand the DoD Information Assurance Certification and Accreditation Process (DIACAP), Vulnerability Assessments, Risk Analysis of Systems, Information Assurance Vulnerability Management (IAVM) compliance, including DISA’s Vulnerability Management System (VMS). Our use of proven IA processes and procedures, along with intimate knowledge of DoD regulations and network operations, provided immediate benefits to our Air Force and Marine Corps customers in the form of increased security posture, streamlined Assessment and Authorization (A&A) projects, and a solid security foundation. Our IA support includes vulnerability scans for STIG compliance, secure reporting of application findings, audit support and support the maintenance of our customer’s Authority to Operate (ATO) and Authority to Connect (ATC).

## 6.5 Task 5 – Cybersecurity (CS)

Our cybersecurity program management approach will ensure coordination of all aspects of cybersecurity in accordance with applicable DoD, DoN, and HQ instructions, policies, and procedures such as DoD Instruction 8500.01. We will work with the CNFJ/CNRJ ISSM and the N6/Region CIO to provide cybersecurity support and manage systems and networks under their responsibility. This includes systems and networks administered in conjunction with NCTSFE staff in the ONE-Net environment. The AveningTech team has managed programs nearly identical in size and scope and will leverage that experience – along with the directly relevant experience of our proposed team members – to continue support to CNFJ/CNRJ with no service interruption.

Subtask 1 – CS Program Management. The AveningTech project manager (PM) will act as the single point of contact for the Contracting Officer (KO) and the Contracting Officer’s Representative (COR) for the overall task order. We have successfully provided similar support for the government on various contracts, most notably our support of USCG’s TISCOM. Our proposed team has provided a range of cybersecurity support functions, many of them directly to CNFJ/CNRJ, and understands the need to maintain records of instructions, directives, guidance, checklists, and policies and procedures, including STIGS. Our personnel are familiar with the OPTEMPO required to perform in the CNFJ/CNRJ environment, as well as the intricacies of the environment itself, and are experienced with the knowledge databases used to store cybersecurity records. We will keep records in hard or soft copy as required by the government. We will provide assistance with generating instructions, guidance, and policies and procedures. We understand the nature of departmental reports and their formats as preferred by CNFJ/CNRJ leadership.

We will leverage our history of support of enterprise-wide tools on the USCG TISCOM cybersecurity SME project (ACAS, HBSS, SCCM, data at rest, data in transit, GPOs, STIGs, and SRRs) in conjunction with our team’s knowledge of their application in the CNFJ/CNRJ environment, to protect all required systems. We will provide advisement, review, and recommendations of cybersecurity processes to support IT and communications projects to the N6 via the ISSM.

Subtask 2 – System/Access Control Management. The AveningTech Team provides system and access control services to our government customers. We help customers minimize risk by performing physical and logical access control to ensure authentication and authorization of users and entities to systems and premises. We process access and account requests for users and act as ISSO, ISSM, and/or ISSM appointees as designated by customers. Our services include processing requests for VPN access, OWA, and firewall exemptions in accordance with applicable security standards. Our access control capabilities include administration for passwords, PINs, biometric scans, tokens, and other authentication factors. We administer multifactor authentication when required.

Subtask 3 – Assessment and Authorization (A&A): We are experienced with assisting federal agencies with conducting detailed and systematic security assessments to achieve and maintain compliance with security standards. We perform these tasks in support of NGEN-R SMIT and PACAF C5ISRO. Our assessment and authorization (A&A) process provides our customers with confidence that their data is stored and processed on secure and reliable systems. We assess system policies, technical- and non-technical security components, documentation, supplemental safeguards, policies, and vulnerabilities. We have assisted our customers with developing policy to determine the purpose and scope of the certification and accreditation (C&A) approach, then conducted system assessments to ensure that security weaknesses and vulnerabilities are exposed before they had a chance to compromise the organization’s systems. In conjunction with our customers, we select security controls based on our assessment and customize the overall security approach. The purpose of our assessment is to determine if the controls are implemented correctly, operating as intended and producing the desired control described in the System Security Plan. We provide a Security Test and Evaluation Plan and a Security Assessment Report. We develop plans of action and milestones (POA&M) and assist our customers with achieving certification letters and accreditation letters.

We are accustomed to being flexible as changes in the cyber security world are commonplace. We also implement NIST 800-94 and Risk Management Framework (RMF) systems, understanding that DISA and NIST guidance requires the government to analyze weaknesses to ensure the most critical security weaknesses and/or the weaknesses identified on systems with the greatest potential impact to the organization’s mission are addressed first. The careful prioritization of weaknesses helps to ensure that critically important weaknesses are allotted resources within a time period proportionate to the risk associated with the vulnerability or system.

In the event that Team AveningTech’s team requires access to the government furnished servers, our IT Section Lead will provide assurance that all IT equipment and programs comply with Government security requirements including RMF and agency-specific compliance. All commercial off-the-shelf (COTS) products that would potentially be installed on the network will be verified for a Certificate of Networthiness (CoN). Team AveningTech understands the processes for identifying software usage and the process for the identification and verification of CoNs. Validating software CoNs is an important step to increasing network and information security. This information will be provided to the Government’s Configuration Control Board (CCB) and will only be acted on with written approval from the board. Additional support will include STIG and policy remediation on required devices, documentation and SOP creation and updates to facilitate RMF compliance of potential equipment within Team AveningTech’s area of responsibility.

If required, Team AveningTech will maintain its applications and firmware to include the latest patches and updates, register all assigned servers and maintain appropriate certifications at all times in accordance with DOD security regulations. We will work with the government to remediate any vulnerabilities and proactively manage application of Security Technical Implementation Guide (STIG) configuration standards to all servers. All systems under the control of the contracting staff will be scanned, patched and maintained at the highest level possible.

Our staff is very familiar with remediation to support the Risk Management Framework (RMF). All software code/interfaces will be analyzed to identify interface issues or integration discrepancies residing with the current software code, documentation, and/or actual system performance. Findings and recommended corrective action(s) will be documented, and upon Government test team approval, accomplished. Requirements changes resulting in changes to existing software will be documented. After testing and validation, the changes will be approved by the appropriate Configuration Control Board (CCB), documented, and integrated into the software baseline.

Team AveningTech embeds information assurance and cybersecurity initiatives across all service offerings, with our risk management processes incorporating ISO 31000 principles. In addition, Team AveningTech cyber security personnel are RMF experts, assisting multiple customers with the C&A process, in accordance with NIST 800-37. We apply RMF in a NIST-compliant multi-step approach Team AveningTech also applies the RMF risk scoring approach in a continuous monitoring environment, which we will embed in DON’s information security program. For success, it requires assessment of all security controls, including management and operational controls that cannot be assessed using automated tools, and therefore requires both automated and manual processes. Team AveningTech is the best choice to implement continuous monitoring in RMF because our approach to the security assessment process is streamlined for DON to reduce the level of effort for system stakeholders. Further, Team AveningTech will fundamentally change cybersecurity’s relationship to the mission by developing and employing an Enterprise Service Delivery Model (ESDM) supported by a flexible, continuously improving program that tailors protection strategies. We deploy automated cybersecurity assessment and reporting tools built to determine cyber risk management capabilities measured against multiple international standards and applicable regulatory guidance. Our risk assessment methodology is anchored in security frameworks that include NIST, ISO, and Control Objectives for Information and Related Technology (COBIT)-5.

Subtask 4 – Audit and Compliance Management: A security audit requires compliance management, and is a systematic evaluation of the security posture of an agency’s information systems by measuring how well it conforms to the established set of security policies. A thorough audit Team AveningTech carries out typically assesses the security of a system's physical configuration and environment, software, information handling processes and user practices. We use process-approved templates, data compliance through integrated validation, policy and regulatory support. Our team uses a range of approaches to minimize vulnerabilities and target many types of cyberthreats. Detection, prevention and response to security threats involve the use of security policies, software tools, and IT services.

Subtask 5 – Incident Handling and Response: The AveningTech Team uses the National Institute of Standards and Technology (NIST) incident response framework to structure and implement our incident handling and response approach. Our approach identifies and mitigates cybersecurity incidents through a several step process, including preparation/anticipation of an incident, detection of an incident, containing the incident, eliminating the threat, and reaching full recovery. We then conduct post-incident analysis and learning to help prevent damage from similar future incidents.

We develop a tailored incident response plan for each effort and will produce one for CNFJ/CNRJ. Our plan features an effective process for identifying an attack, determining its potential severity, mitigating it, restoring operational activities, and preventing further occurrence. With the understanding that incident prevention is everyone’s responsibility, we involve all team members in our incident response team in some way. As there are no dedicated incident responders for this CNFJ/CNRJ effort, we will fill incident response roles with existing team members who have other technical roles. Service disruption is a risk we have accounted for, as described in our response workflow and incident response time prioritization.

Team AveningTech technicians often find knowledge base system embedded in the ticketing system a huge asset. Knowledge based systems allows Team AveningTech to capture, reuse and maintain documented IT solutions and expertise. The repository serves as an immediate research tool with solutions that were successful on the network we are supporting. We have available to us step by step resolutions for common service requests and incidents. This helps in providing quick, consistent service and increases chances of first call resolutions. Response times for individual task areas will mirror the requirements stated on page 175, etc., of the RFP PWS. Service call response and completion times will cover the specific tasks for C3P Ashore Support; Enterprise/Infrastructure Services Support; CS Support; Managed IT Services Support; and, Bilateral Communications and Networks Management Support.

|  |  |  |  |
| --- | --- | --- | --- |
| **Severity Level** | **Response Time** | **Description** | **Resolution Time** |
| Critical | Within 15 minutes | Complete outage, multiple users impacted, no immediate workaround | Within 8 hours |
| High | Within 1 hour | Degraded service, multiple users affected, latency issues, unable to log into systems | Within 12 hours |
| Medium | Within 8 hours | Does not immediately impede mission performance, only one user affected, work arounds exist, break/fix request | Within 3 business days |
| Low | Within 1 business day | Equipment upgrade, move, new component or enhancement. Impact is low and work can be scheduled based on business case | Within 7 business days |

On-call service will be provided, with access to our technicians via their company-provided cell phones during both regular and non-business service hours. As part of our quality assurance process, AveningTech incorporates a formal lessons-learned process throughout the life of our projects included in our internal quarterly program reviews. We have found that conducting overarching lessons learned reviews at periodic intervals serves as a basis for new and innovative solutions for our clients. Our PM schedules formal lessons learned meetings on a quarterly basis to include members of the AveningTech team and all relevant stakeholders in the customer organization. Results are formally documented and shared with all parties involved and are included as part of a Monthly Status Report.

Our PM will act as the overall incident response manager who coordinates incident response team activities leading up to and during an attack and recovery. Our PM will delegate responsibilities to other de facto incident response team members by assigning them roles related to security analysis (reviewing alerts and identifying and researching potential events) and threat research (providing contextual information around a potential threat). During all phases of incident response, our PM will keep the COR up to date with the latest information in real time.

We borrow from the established NIST incident response lifecycle’s four-step process to design our incident handling and response approach. The NIST lifecycle model is well-established and recognized as an industry standard, so we feel no need to “reinvent the wheel.” The lifecycle’s four steps are preparation; detection & analysis; containment, eradication & recovery; and post-incident activity.

Our tailored incident response plan for CNFJ/CNRJ will feature steps based on the NIST incident response framework. For ***preparation***, we will compile a list of networks under our purview, including all components, subcomponents, servers, and endpoints. We understand that all CNFJ/CNRJ assets are critical and hold sensitive data, so all assets will be treated with equal importance. Our ***detection and analysis*** steps include constant collection of data from all systems, assets, and security tools to identify and anticipate future threats. We will work to understand baseline system behavior so that abnormalities and anomalies in system behavior are immediately apparent during an attack. In the event of an attack, our ***containment, eradication, and recovery*** steps include smothering the attack before it has a chance to pervade the system and cause further damage. We will help CNFJ/CNRJ maintain operations and avoid service disruption by keeping as many critical services available as safely possible during an attack. We will identify the attacking host and block communications to and from its IP address as well as other communication channels it may be using. We will then move to remove all remaining elements of the incident from the CNFJ/CNRJ environment by mitigating malware, closing affected accounts, and/or resetting user passwords and permissions. Our ***post-incident activity*** is critical because it leverages lessons-learned from previous attacks to prevent similar future incidents. Our experienced security professionals investigate each incident, log its particulars, and build a detailed report for the COR and for our future reference. We analyze what happened and how we responded; what could have been done to prevent it; which incident response techniques, if any, did not successfully contribute to mitigation; what new precursors or indicators were discovered; and what tools could be used to mitigate similar issues.

Subtask 5 – Incident Handling and: The AveningTech Team will provide incident handling and response services to CNFJ/CNRJ. We will work with personnel at all levels (users, ITRs, the Security Manager, and any required commands and military branches to respond to incidents. To mitigate the potential risk of incidents, our incident handling and response process includes detection and identification of an incident to determine the nature and characteristics of the incident. Team AveningTech works to determine the potential damage by identifying the type of threat (data theft, a network breach, etc.). We determine the potential severity of the threat and which systems are likely to be affected.

We identify and quarantine any discovered malware and conduct interviews of event witnesses and any personnel involved to gather more information for mitigation and lessons learned. Team AveningTech removes all artifacts of the incident from all systems, work with CNFJ/CNRJ to repair and/or update system(s), verify currency of all security patches, and verify validity of system backups. We are careful to conduct continuous monitoring and testing of all systems for remaining vulnerabilities or new threats caused during the incident. Finally, we conduct assessment of the event or incident which includes step-by-step accounts of what occurred, what steps we took to contain the incident, who was involved, descriptions of the threats discovered and remediated, which personnel were involved (or accountable), and what future actions CNFJ/CNRJ and the AveningTech Team need to prevent similar events from happening. In support of the USCG TISCOM, NGEN-R SMIT, and PACAF C5ISRO programs, the AveningTech team has responded to a range of incidents and violations while successfully remediating threats and reporting to appropriate command officials. We understand that not all threats are conducted by malicious actors and that many incidents are unintentionally committed by well-meaning members of the command. In such events (USB violations, software violations, web/proxy violations, PII leaks, and classified spillage), we work with the command to respond while maintaining and reiterating to personnel at all levels the importance of insider threat awareness.

Team AveningTech has a full range of experience in cyber security to cover Subtask 6 through 10. Team AveningTech provides vendor-independent and DOD branch-specific audits against known cybersecurity and data protection threats, which includes endpoint protection for Non-classified Internet Protocol (IP) Router Network (NIPRNet)/SIPRNet users, audit of user rights, and access levels. We also carry out IT cybersecurity CS/IA Awareness and Training workshops. Inspections, Assessments, and Visits, We support Public Key Infrastructure (PKI) and Site Trusted Agent (STA) and Workforce Management.

## 6.8 Task 8 – Cyber Threat Security Plan

With experience managing Controlled Unclassified Information (CUI) that requires safeguarding or dissemination controls, our team drafts SOPs pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended, as well as specific DoD requirements. Non-public information handling may include information sharing — making information available to appropriate personnel (people, processes, or systems) so that stakeholders may leverage information held or created by another party, but is of a non-public nature. Our team understands DoD Instruction 8170.01 and DoDI 5200.48, and these direct our handling of non-public information consistent with the government’s needs and requirements. For example, in accordance with the DoD phased 11CUI Program implementation, all documents containing CUI must carry CUI markings. Our security SOPs will be submitted for review, and are consistent with the CUI handling guidelines issued through the Information Security and Oversight Office (ISOO) as Part 2002 of Title 32, CFR, which provides implementing requirements for E.O. 13556.

Team AveningTech will draft a cyber security plan that (as the primary deliverable) updates and clarifies the security policies, procedures, and controls required by the government to protect the client against threats and risk. Our cyber security plan will also outline the specific steps to take to respond to a breach. The plan will address Vulnerability Management such that it evaluates network components, security procedures, and processes for potential exploitation from attack. Other sections will include Cyber Threat Intelligence; Analytics Monitoring; Mitigation and Response; and, a Lessons Learned and Action Plan to provide lessons learned and an action plan that will help all interested parties avoid repeated and similar attacks. The teammates will be required to implement this requirement within their processes in support of this task. Annually, we will verify with our teammates and the Contracting Officer and COR that the plan remains valid.

Our approach to developing the plan starts with conducting a Security Risk Assessment following the RMF guidelines from NIST and DoD. We then will work with stakeholders to set security goals. The team’s cyber experts will then evaluate current and planned technology, and recommend the appropriate changes to the security framework, after a review of existing security policies. As discussed in the previous section, we will then create a draft Risk Management Plan. Once reviewed and approved, Team AveningTech will assist as needed to implement the recommended security strategy. With the need to respond to a changing threat landscape, we will periodically evaluate the security strategy and make on-going recommendations.

# Subfactor Two - Program Management

Team AveningTech’s approach to project management is based on the principle that effective communication is the key to performance and customer satisfaction on services contracts. We employ dedicated program management resources who directly engage with our clients, and respond rapidly to ensure that we are providing high-quality and consistent support. Our proposed candidates for CNFJ/CNRJ are reliable and many have a demonstrated history of support on this program providing response and completion within the stated limits. Their redacted résumés are presented in the appendix. Should the Government change requirements for response and completion times we will adapt to the new standards by ensuring all contractor employees are briefed and provide acknowledgement of the new requirements. We will ensure that whether a problem (1) arises during normal business hours or other than normal business hours; (2) results in work stoppage or no work stoppage; (3) results in system degraded or operational; or (4) renders a system or systems unavailable, the AveningTech team will be available within the stated, required time limits to complete the service call and provide appropriate status to GR.

The Team AveningTech program management plan includes provisions for providing fully qualified, appropriately certified personnel who can meet all PWS requirements as stated in Paragraph 13.2.9 Qualifications. Our staffing plan is laid out in greater detail later in this volume and names specific candidates for each role, where they will work, and what PWS tasks they will be responsible for. Our staffing plan and labor mix is reflected in this volume as well as our cost volume, where we lay out a labor category mix, all required hours, and other direct costs.

Managing geographically dispersed employees who are co-located on or travel to client sites relies on robust and consistent communication between staff, subcontractors, and management and client representatives. In cases where there are multiple employees in a single location, we often identify a site- or team-lead, who becomes the local supervisor and primary point of contact, interfacing with the local client organization and with AveningTech management. In cases where there is a single employee at a designated location, we put extra emphasis on evaluating candidates to ensure that those selected are able to work independently with remote supervision. Managers and supervisors travel to client sites as often as possible to meet with employees and client points of contact to ensure that the support provided is consistent with contract requirements and customer expectations.

On other engagements, our PM is responsible for staffing, budgeting, scheduling, client interaction, reporting and issue resolution, and is the primary point of contact for the Contracting Officer. Our key project management personnel ensure efforts comply with all terms of our contracts, including ensuring staff training is up to date, security requirements are adhered to, and accurate invoices are submitted in a timely manner. The PMP includes well-defined project controls that are updated regularly, ensures each requirement is staffed with qualified and responsive personnel, provides standard operating procedures to ensure consistent reporting and Continuous Process Improvement (CPI), and integrates and standardizes program controls and project planning processes.

Our formal, well-established project management process address preliminary planning through closeout to develop the overall skill mix, level of effort, specific tasks, and define the overall performance objectives. Upon award, Our PM schedules a kickoff meeting with the project team and client stakeholders to review goals, objectives, roles, responsibilities, requirements, deliverables, milestones, schedule, budget, assignment parameters, and success factors for each engagement. Based on input from this initial meeting, the PM adjusts the overall staffing plan and tailors our tools to enable the optimal labor mix for the task. Our proposed PM for this effort has direct, relevant experience with CNFJ/CNRJ to include the design, planning, and implementing technical Cyber Defense and Incident Response solutions for the OCONUS Navy Enterprise Network (ONE-Net) providing services to all U.S. Navy ashore users in the USINDOPACOM AOR. He has developed and implemented countermeasures for adversary Tactics, Techniques, Procedures (TTPs), and indicators of compromise (IOCs) as well as performing detailed cyber analysis on all network and endpoint related cyber events occurring in the ONE-Net Far East region to include packet flow, PCAP, dynamic malware analysis (sandbox execution), and event correlation across myriad cyber security solutions.Management Plan

AveningTech’s management plan is based on the principle that effective communication is the key to performance and customer satisfaction on services contracts. We employ dedicated program management resources who directly engage with our clients, and respond rapidly to ensure that we are providing high-quality and consistent support. AveningTech takes great care in the selection of teaming partners for contract engagements to ensure that our team is fully capable of addressing the scope and level of effort of an engagement. Given our expertise of Navy IT Infrastructure, DON Cybersecurity and RMF principles, along with our unique experience and in-depth knowledge of NMCI/NGEN systems and platforms, ActioNet is that partner! ActioNet provides 18+ years of experience implementing Cloud, Software, System, Cyber, IT Operations, and DevSecOps Engineering services for Outside the Continental United States (OCONUS) and Continental United States (CONUS) large-scale DOD programs.

AveningTech leads a team augmented by two capable specialist firms who provide complementary services to DOD. Teammate ActioNet is a woman-owned large business with 24 years of IT experience implementing Enterprise Infrastructure, Cybersecurity, ITSM, Application Development, IT Operations, Cloud, and DevSecOps Engineering services for Outside the Continental United States (OCONUS) and Continental United States (CONUS) large-scale DoD programs. Certified as an ISO 9001, ISO 20000, ISO 27001, and Help Desk Institute (HDI) Support Center company, as well as CMMI Maturity Level 4 (v1.3) Accreditations for both Services and Development.

AveningTech chose Commdex as a teammate because, with 20 years of mission critical communications experience in all 50 states and in many countries across four continents globally, Commdex is a leading systems integrator in the mission critical telecommunications space. Commdex’s in-house technical expertise covers a broad range of communications technologies and platforms across 4G/5G networks, fiber optic, satellite, and microwave that are widely used across critical communications systems. With experience on over 300+ LMR communications systems including nine large LMR programs each with 100+ sites, Commdex understands what is involved in designing large tactical communications projects and provide the resources to bring exceptional expertise. Commdex is an ISO 9001:2015 and TL 9000 certified organization that has developed extensive quality processes incorporated into every step of the design and deployment process to ensure the highest levels of quality for every one of our systems.

AveningTech takes great care in the selection of teaming partners for contract engagements to ensure that our team is fully capable of addressing the scope and level of effort of an engagement. The AveningTech senior management team has significant experience successfully operating as a prime contractor and have all assembled and managed teams comprising both large and small business subcontractors and teammates. Our relationships with service and product providers extend throughout industry and academia and enable us to assemble teams composed of the most effective mix of skills and experience for each specific program. We continuously develop and nurture positive relationships within industry, and frequently re-partner on subsequent and follow-on engagements.

## 6.1 Task 1 – Task Order Management Support

The AveningTech team will provide an on-site task order project manager (PM) to act as the principal point of contact (POC) for all activities in support of CNFJ/CNRJ. Our PM will receive tasking and technical direction directly from the COR and distribute work assignments to contractor personnel; manage tasking progress; monitor contractor performance; and report back to the COR for all ongoing and upcoming tasking. Our PM will prioritize tasks and break out assignments across the contractor personnel to ensure evenly distributed workload with tasks being assigned specifically to the personnel with the requisite skills and experience to accomplish those specific tasks. Our PM will take direction directly from the government regarding work standards and ensure that those standards are met by contractor personnel through constant evaluation and proactive communication. We will develop program and tasking schedules with government oversight and staff our personnel against those schedules as necessary to ensure required work is done on-time or early.

Our initial and annual refresher training is tailored to government policies and procedures for each specific customer and each specific worksite to ensure that our personnel are always abreast of government policies, purposes, and goals. Our PM will be responsible for ensuring that all contractor personnel are aware of — and in compliance with — specific rules, regulations, and policies.

Immediately following the contract start date, our PM will deliver to the government a draft Task Order Management Plan (TOMP) which describes in deep detail our management approach, description of controls in place to ensure effectiveness, which resources will be deployed (including when and how), and a thorough breakdown of deliverables with due dates. We will tailor the draft TOMP based on government feedback to ensure that the final TOMP is published and in place within 30 days of the contract start date.

Our transition-in plan will contain explicit goals and timelines for putting contractor personnel in place (including any retained incumbents), conducting site-specific training, ensuring badging and access control are taken care of, and ensuring a smooth transition in all task areas by transferring specific knowledge in: Project management information (including POCs, technical documentation, ongoing schedules and milestones, and tasking status); coordination between incumbent personnel and incoming members of the AveningTech team; and administrative information such as policies and procedures, hardware/software inventories, and site access.

On a monthly basis, and on the 10th workday of the month, our PM will provide the Contractor’s Progress, Status, and Management Report. Our report will include financial tracking, narratives of the work completed by the AveningTech team during the reporting period, a description of significant events and/or issues, and upcoming/anticipated work for the following period(s). The Contractor’s Progress, Status, and Management Report will be comprehensive but we will ensure that no information included in the report is a surprise to the government; our PM will ensure proactive, honest, and timely communication with the government on any and all issues (significant or insignificant) far before the official report is delivered on the 10th workday of the month. Our PM will ensure that the COR is abreast of all pertinent contractor reporting content on an ongoing basis; our monthly report will simply codify the information for official record.

All projects start with the creation of a Project Management Plan (PMP) that contains standardized artifacts and a WBS tied to the task order deliverables. Team AveningTech has embraced a company-wide delivery methodology and practices continuous process improvement and the lessons learned from each Team AveningTech project are reflected in successive evolutions of the delivery framework. Our on-line project management portal will be a repository for all task order directives, draft deliverables, schedule management, and other tools to support execution of the government’s requirements.

This task order is controlled using Team AveningTech’s PMBoK-based methodology, Team AveningTech’s approach to project management is a hybrid, which implements our ISO-based Project Delivery Framework, consistent with Project Management Institute (PMI) best practices. Our framework is compliant with CMMI Level 3 for project/task management and uses Team AveningTech’s standardized Project Management Plan (PMP) template, which is followed to plan, monitor and control the work, and meets the specific requirements of this task order. We integrate our delivery framework and tailor it to our client’s project planning requirements and existing practices to consistently deliver projects on time and within budget.

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

Team AveningTech will support CNFJ/CNRJ by maintaining an experienced, on-site, IT contractor team capable of providing C3P Ashore operational communications, situational awareness, and mass notification requirements. Team AveningTech will follow current procedures and processes in place to support established C3P Ashore enterprise and operational communications requirements in compliance with CNIC Instruction 5222.1. The AveningTech team has current and past experience doing similar Operations Center support in Japan, Hawaii, Guam, Italy and several locations detailed below. We will provide tactical-level support for the staff, including operations center system communication suites, mass warning systems, contingency satellite communications equipment, and virtual/telework capabilities/infrastructure for the key members of the crisis response organization. We will leverage our experience to effectively manage C3P workload in compliance with CNIC Instruction 5222.1 . For the Commander, Navy Region Hawaii (CNRH), team member ActioNet provided on-site technical, telecommunication, logistics, networking, information assurance and administrative services in the following areas:

* Telecommunications- Telephone Control Office (TCO) - Provided support for fixed and wireless voice services, dedicated transmission services, and cable television services. Provided inventory management, usage validation, and maintains a customer database.
* Telecommunications (TCO)/Information Assurance (lA) - Provided technical support for TCO taskings with an emphasis on information assurance and information security in telecommunications systems in the Navy Region and Joint Base IT TCO/IA Branch N64.
* NMCI Customer Support - Provided technical support for the Region IT NMCI Contractor Technical Representative (CTR). Assisted in seat management for the Navy- Marine Corps Intranet customer support services, including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements.
* IT Logistic support - Responsible for maintaining and tracking the CNRH Regional Inventory Tracking Application (RITA) database. Tracked the disposition of all IT equipment not belonging to NMCI. Responsible for the maintenance and inventory of IT equipment. Deployed classified equipment upon demand and situation requirements.
* Land Mobile Radio (LMR) - Provided technical review and draft white papers or project analysis for Pacific Land Mobile Radio (PLMR) supported functions. Provided solution and coordination for CNRH PLMR projects. Supported PLMR technical requirements for unit programming; talk group management etc. in line with established Government policies and directives. Provided project coordination for PLMR related services - includes customer, vendor, and inter/intra Government coordination. Completed service validations, site surveys, data calls. Developed and maintained inventories and responded to data calls. Assisted with PLMR asset and circuit equipment validations. Maintained and managed the LMR database in accordance with Government's tracking requirements.

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

Team AveningTech offers an approach that will overcome significant challenges to the Navy Program, which requires 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 will 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 AveningTech has the capabilities to meet these challenges and has demonstrated experience supporting various C3P systems for multiple agencies.

Subtask 1– ROC/EOC/RDC/LDC Support. We understand that 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 AveningTech 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.

Subtask 2 – Emergency Communications Support. Team AveningTech 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.

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

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

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 AveningTech 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 fleet mapping 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.

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

In delivering managed IT services, all of our work is performance based, and conducted under quality processes and frameworks as adopted by the customer, or using our own ISO, ITIL, or CMMI ready-to-deploy processes to provide service support that yields desired objectives through goal recognition, assignment of relevant measures, and metrics collection, analysis, and reporting, Team AveningTech has demonstrated our approach to managing workload with an eye on desired outcomes works well — we have delivered Entry Control Point and Access Control Systems (ACS) support successfully for the Navy and other DoD branches.

## 6.3 Task 3 – Enterprise/Infrastructure Services Support

Team AveningTech draws on our significant experience and expertise operating large ­scale IT Support and Service Desk operations for our federal customers and determining most efficient and optimum staffing levels. Our approach delivers on several key elements, starting with seamless transition with no disruption to the mission. With over a dozen successful transitions (most within 30 days) , as demonstrated in our Transition Plan, we provide for effective and efficient knowledge transfer. Our managed IT services are based on established Service Desk ITIL ­based, ISO ­certified processes and procedures that comply with Help Desk Institute (HDI) best practices. This proactive approach will meet and consistently exceed SLAs that we establish with the government — and constant SLA monitoring and establishing proactive remediation before thresholds are reached can be assured. As for expert personnel, Team AveningTech ensures initial and periodic refresher training and monitoring for any chronic staff issues that would trigger an upgrade of staff. Our Service Desk operators apply innovation directly into appropriate Service Desk tool without going through a third party. This means we provide cost efficiency through innovation, automation, and efficiency.

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 data centers 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).

6.3.2 Subtask 2 - Application Strategy 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.

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, teaming partner ActioNet 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).

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 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.

For the DOE ITSS we utilize MS SharePoint, ServiceNow, Bomgar, Apropos, and Wiki to provide consistent, automated, and quality support, templates and workflow of requests, incidents, problems, knowledge articles, change requests, assets, configuration items, service level targets, reports and dashboards. Technicians are trained in the proficient use of the tools. The benefit to the government is accelerated solution delivery, improved customer responsiveness, improved cost estimating and monitoring on-time solution delivery, incorporation of industry best business practices: e.g., CMMI, ISO.

6.3.3 Subtask 3 - Operational Application Management. For NIWC LANT, teaming partner ActioNet worked closely with technical service managers (TSMs), using NMCI Enterprise Tool (NET) to manage 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 enterprise approved software. All utilized hardware/software maintained 100% compliance with Department of the Navy Applications and Database Management System (DADMS). ActioNet provided over ten years of IT infrastructure and application management support for National Oceanic and Atmospheric Administration (NOAA). NOAA provides a deep understanding of weather and climate platforms such as National Environmental Satellite, Data, and Information Service (NESDIS), Advanced Weather Interactive Processing System (AWIPS), and National Centers for Coastal Ocean Science (NCCOS).ActioNet provided all personnel, management, equipment, tools, maintenance, materials, supervision, documentation, processes, and non-personal technical support services necessary to perform Application Management Services (AMS) services and satisfy daily AMS activities, administration, process advancement, objectives and standardization within each AMS functional area.

3.3 Subtask 3 - Operational Application Management. Team AveningTech’s cost-cutting, quality-improving 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:

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

## 6.4 Task 4 – Enterprise Architecture

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. Our team will provide portfolio and knowledge management, including portal content development and implementation in support of CNRJ / CNFJ and its installation sites. This will be in accordance with guidance provided by CNIC and higher authorities. 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’s 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 and 6.4.2 and Subtask 3 - Portfolio Management Liaison Support. Team AveningTech will be responsible for customer assistance with portfolio management, software lifecycle management and periodic DADMS and DIPTR-DON review. By taking the time to plan, configure, and document activities to collect a “project-of-projects,” we facilitated portfolio management actions leading to effective lifecycle management and carefully managed Return on Investment (ROI) decisions. Our deliverables are built and support organizational process improvements that lead to success in infrastructure availability and capacity. We provided Tier III expertise when self-service was insufficient, and technicians escalated the service request. This was across all enterprise systems — so Team AveningTech needed a “30,000 foot” view of the portfolio to support the client’s programs.

In adopting ITIL Service Portfolio Management as our approach to manage the service portfolio, Team AveningTech ensures that the right mix of services are available to meet mission requirements so outcomes come at an appropriate level of investment. Team AveningTech will maintain DADMS / DITPR-DON records and its related files for all systems/networks under the responsibility of CNFJ / CNRJ. Team AveningTech will provide DADMS / DITPR-DON support as region portfolio manager. Good communications skills, both oral and written, are necessary, as there will be considerable interaction with customers, vendors, Echelon II staff, and other stakeholders in support of these systems. 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.

6.4.2 Subtask 3 – Portfolio Management Liaison Support. Team AveningTech will provide expert support for systems which CNRJ / CNFJ holds a responsibility. We will provide portfolio expertise to manage any which are administered in conjunction with NCTSFE staff within a ONE-NET environment. Team AveningTech will liaise with the appropriate personnel for ONE-NET to ensure above-baseline software approval. We are experienced with managing licenses for custodians to validate compliance, request ONE-NET to authorize new software to be approved on ONE-NET. Team AveningTech will conduct research into the latest software release of the CNRJ / CNFJ and its installation site so utilized software will comply with DOD / DON software standards. Our technologists will advise on a software migration plan to comply with DOD / DON standards as part of our security assessment or whenever necessary.As the prime contractor, AveningTech provides Technical Support Services to the I MEF G-6 section by providing an information technology integration team in support of I MEF operations in garrison and tactical environments. Support services for the Microsoft Office 365 applications enable greater capability and utilization as I MEF and the USMC fully utilize cloud platform services. In addition, these efforts reliably integrate command, control, communication, and computer (C4) systems and support information exchange requirements across the I MEF CE and Major Subordinate Commands (MSCs) and provide staff support on Command and Control (C2) system operations, coordination and execution in support of the Marine Air Ground Task Force (MAGTF).

Our team is experienced as Command and Control Systems Integrators. We support the staff sections by coordinating and de-conflictingC4 systems integration with higher, adjacent, and supporting organizations within the Department of Defense which may affect the MAGTF command and control network and critical systems as defined by I MEF stakeholders. This means we discover, request, and maintain C2 systems ports and protocols for pertinent MEF C2 systems and coordinate requests within the I MEF G-6. Our experts support and assist in the integration of warfighting systems within I MEF to support  
operations and exercise objectives to include but not limited to ensuring network firewalls and virtual local area networks (VLAN) are established to enable C2 systems functionality on garrison and tactical domains.

Members of the AveningTech team support and coordinate with I MEF staff sections to support project management for C2 systems and information technology in support of garrison and tactical functions. The team provides recommendations to align and prioritize resources, assets, and shall coordinate directly with each staff section to understand each staff’s C2 application requirements to include programs of record Joint Tactical Common Operational Picture Workstation (JTCW) and Tactical COP Server (TCS).

We also coordinate with the staff sections to help sections identify and prioritize information exchange requirement and pertaining systems that support each phase of an exercise/operation supporting Command and Control in a Denied or Degraded Environment (C2D2E). Team AveningTech supports development and execution of appropriate Information Management Concept of Operations (CONOPS), plans, and annex U. Provide governance and oversight on the employment and integration of C2 systems in accordance with I MEF techniques, tactics, and procedures (TTP). Our experts advise on the creation of Technical Directives (TECHDIRs) and Operational Directives (OPDIRS) to assist with the de-confliction of the C2 communications architecture.

## 6.6 Task 6 – Managed IT Services Support

As part of the Region and Installation IT staff, Team AveningTech is providing personnel to support service delivery based on the Information Technology Infrastructure Library (ITIL) frameworks. We are experienced at web, database, and specialized application support. We will also support other Departments in the migration or implementation of CNIC enterprise IT initiatives, web or portal sites and application software as required.

Subtask 1 – CNIC and ONE-NET Liaison Support: AveningTech is providing a range of support to NGEN —and has been for nearly a decade. Our support of PACAF C5ISRO is also directly relevant; AveningTech has provided these types of services to multiple military branches. CNRJ/CNFJ General ONE-Net liaison support includes coordination with ONE-Net/NGEN TNOSC/Cyber Security personnel to ensure that CNRJ/CNFJ ONE-Net systems are in compliance with Naval Network Warfare Command ONE-Net Information Bulletins (OIB). We maintain command assets management list and perform annual inventory and validation. We catalogue and report annually on physical security STIG requirements ISO ONE-Net assessment and authorization efforts. Demonstrating a clear understanding of the requirements for storage/file types for command shares and provision/monitor the appropriate command file share configuration(s), we catalogue and conduct annual validation for authorized removable storage devices to ONE-Net Cyber Security stakeholders. Our technicians handle the request, track, and authorization workflow for the use of authorized USB wireless capabilities, embedded web camera and microphone capabilities. We put in place SOPs for moving/relocating ONE-Net systems and coordinate system changes with the appropriate ONE-Net stakeholders.

To provide CNRJ/CNFJ Cyber Security ONE-Net liaison support, we conduct local cyber security training for CNRJ/CNFJ ONE-Net users; provide local cyber incident response review and resolution with ONE-Net Cyber Security stakeholders; ensure physical spaces meet security requirements for processing classified data/housing classified systems; and, provide artifacts for CNRJ/CNFJ spaces/configurations ISO ONE-Net assessment and authorization efforts. ONE-Net provides KMI services to CNRJ/CNFJ who is a local element to NAVCOMTELSTA FAR EAST. CNRJ/CNFJ coordinates all KMI services with the ONE-Net KMI team ISO cryptographic devices in use at CNRJ/CNFJ. CNRJ/CNFJ hosts multiple Community of Interest (CoI) and Program of Record (PoR) systems that utilize ONE-Net/NGEN network infrastructure and/or services. These CoI/PoR systems can be non-complex (e.g, only receive network infrastructure) or complex (e.g., receive network infrastructure and other ONE-Net/NGEN services such as HBSS (Host Based Security System), DNS, authentication, file sharing).

Subtask 2 – Systems and Network Support: In support of PACAF C5ISRO our personnel are appointed as Information Systems Security Officers (ISSO) for the Pacific Enterprise Service Center’s (PA-ESC) Area of Responsibility which includes three Numbered Air Forces (NAFs) and ten bases in the Pacific. We provide expert level system security analysis and associated services supporting assessment activities conducted by the Air Combat Command/A26 at each stage in the lifecycle to ensure delivery of an accreditable Air Force Joint Worldwide Intelligence Communications System (AF JWICS) for the Pacific theater and all three NAF subordinate commands and ten bases in accordance with Intelligence Community Directive (ICD) 503. We ensure compliance with Office of the Director of National Intelligence information security requirements including compliance with all ICDs, STIGs, and other documented security requirements for AF JWICS, mission systems, and weapons systems through all phases of the lifecycle.

On NGEN-R SMIT we conduct Marine Corps Enterprise Network (MCEN) Unclassified and classified LAN/WAN/NOC network administration of over 1500 Cisco and Enterasys switches and routers in a highly available (HA) environment. Perform site surveys, design, and install network infrastructure solutions for new and expanding customer installations. Monitor and troubleshoot all boundary devices enterprise wide, for Marine Corps Cyberspace Operations Group (MCCOG). Provide course of action, resolution, documentation, and processing of tickets using the BMC Remedy IT Service Management console.

For NGEN, AveningTech technicians perform Active Directory, Exchange, Blackberry Enterprise Server and BUEM, Virtual Infrastructure (VMWare) and SAN (NetApp) administrative tasks in support of MCIEAST and MCCOG product group specific requests/incidents. On NGEN-R SMIT we provide platforms support to the team by building out domain controllers, making DNS modifications and updating Active Directory Sites and Services for new installs/modifications. In this role, we participate in daily task meetings via WEBEX in which tasks are assigned/completed in JIRA. We support the MCCOG EDM Platforms Tier III team by working requests assigned by their leadership and participating in their meetings on a weekly basis. This support includes resolving incident requests, work orders and change requests that are assigned to the EDM Platforms Tier III team in the MCCOG Remedy system. We ensure that all Platforms servers are compliant to IA scans and assist in remediating any findings. AveningTech team members provide local tier III support as members of the MCCOG Det EDM Triage team at Camp Lejeune. In this role, we function as touch labor for various MCCOG EDM teams to provide support to our enterprise infrastructure that is in our local area. Additionally, we provide escalated support for any issues that arise in the MCIEast AOR prior to escalating them further up the ladder to MCCOG in Quantico.

Subtask 3 – VTC Support: AveningTech network engineers provide hardware maintenance design, installation, and support for PACAF VTC systems in Hawaii, Alaska, and Japan. Post-installation services include remedial maintenance, preventive maintenance inspections, repairs of critical system components within 2 hours after notification when spares are available, repairs of non-critical system components within 7 days of receipt of spares conducting acceptance tests of repaired items in accordance with the Acceptance Test Procedures (ATP) established by the Original Equipment Manufacturer (OEM) or in accordance with a site-developed validation and verification process approved by the on-site COR; performing fault isolation (troubleshooting); removing faulty equipment and parts; and relocating equipment components to support facility reconfigurations. Our team will be responsible for scheduling routine equipment maintenance, performing equipment and connectivity troubleshooting, and processing trouble calls (see the Quality Assurance section of this document).

We provide meeting support by planning and arranging for conferences, meetings, preparing training and presentation materials (PowerPoint, video, or presentation posters) and recording and disseminating minutes; development and tracking of correspondence, reports and briefing materials; and, via our on-line portal, maintenance of a document library. Support that Team AveningTech provides also includes researching and providing recommendations on best practices to improve areas within Program or Portfolio Management; evaluating issues and providing recommendations related to program cost, schedule, and performance; and, providing analysis and re-commendations.

Subtask 4 – Asset Management Support: AveningTech provides end-to-end lifecycle support for government information technology equipment. We assist our customers with ensuring that their computers, peripherals, and other assets are properly tracked through the lifecycle, are loaded with current firmware and software, are maintained to industry standard, and are repaired or replaced on appropriate schedules. Our personnel fuse their expertise in systems engineering with knowledge and understanding of government asset management best practices to provide our customers with confidence that their assets will be fully mission capable and ready to support operations with minimal downtime.

In support of NGEN for the Marine Corps Cyberspace Operations Group (MCCOG) Marine Corps Enterprise Network (MCEN) Integration Branch on Marine Corps Base Quantico, our technicians serve as asset and configuration management Subject Matter Experts (SME) for the Domain Consolidation & Elimination (DC&E) Project, which is a USMC mission initiated to collapse and eliminate existing legacy domains into a single MCEN-NIPR management domain. We are responsible for populating migrated legacy end user, server and network infrastructure devices into the Remedy Atrium Configuration Management Database (CMDB) and modifying Configuration Items (CIs) as necessary to ensure accuracy. We analyze and inventory key network infrastructure assets for planning of enterprise infrastructure migration and upgrade while collaborating with over forty legacy domain Asset POCs to ensure the import and configuration of asset records within the Remedy CMDB were comprehensive and precise. To facilitate asset management, we constructed Excel macros to process site discovery analysis data for swift asset record import into the Remedy CMDB Templates.

We provide physical inventory support at the Command’s preferred interval (typically on a monthly basis). We prepare a physical inventory form from the current program property list (property book) and conduct a wall-to-wall physical inventory in conjunction with the government customer. We take note of any discrepancies with asset location, model number, serial number, or other unique identifier, and immediately update the property book at the completion of the inventory cycle. We report our findings to the Command immediately upon completion of the inventory cycle, highlighting any discrepancies or inventory anomalies. In the case of a missing asset, we conduct an investigation to determine its whereabouts using the asset’s paper trail and conduct a loss report if necessary.

When assets become outdated, unsupportable, or are damaged to beyond economic repair (BER) status, AveningTech prepares disposition paperwork and executes delivery of unwanted assets to the Defense Reutilization Management Office (DRMO) or other disposition authority as directed by the Government customer. Our engineers track equipment warranty through the asset lifecycle to facilitate replacement and repair. As requested by our government customers, we conduct cost/benefit analyses to provide recommendations on warranty renewal or cancellation based on any given asset’s status (age, level of repair, criticality, cost to replace, or other factor). When the Command’s asset management or inventory control system features warranty tracking capability, we ensure that all warranty data is current for each asset in the property book.

Our engineers work hand-in-hand with our government customers to develop plans for upgrading or replacing certain infrastructure on a regular schedule (tech refresh). Antiquated technology leads to lagging performance and service delivery and difficulties with predicting energy and space consumption costs, which increases administrative overhead costs. To reduce maintenance costs of IT assets and reduce risk of costly failures, we help our customers look forward to the next generation(s) of infrastructure support with the specific goal of limiting the variation in computer make and model to streamline service center support, minimize hardware sparing cost, and facilitate the replacement process.

To support tech refresh, our engineers identify availability of information assets, maintain data for the transition of old to new work stations, assist in disposition of legacy equipment, coordinate tasks with Service Provider, maintain data for the transition of old to new work stations, create Active Directory records, and assist with the disposition process for equipment subject to tech refresh.

Subtask 5 – Telephone Control Officer (TCO) Support: The TCO serves as a focal point for the maintenance and management for all telephone material and equipment requests. We will be responsible for the submittal, tracking and processing of all service requests. This includes accepting support requests from staff members and insuring they are complete after determining if such requests are within budget/policy requirements. Team AveningTech will maintain a database of all land-line phones used by the command, along with functionality documentation, and will provide any training refreshers. Our TCO will assist N6 TCO in accepting requests for Telephone Service Requests (TSRs), tracking documentation, and pre-validating requests using command guidance from OPNAVINST 2100.2A. With our history of exception customer service, the government can be assured than interactions with the Base Communications Office and customers with TSRs for renovation and relocation will go smoothly.

Subtask 6 – Life Cycle Management: Team AveningTech will provide bill-of-materials (BOMs), repair estimates and other services as required by the Government representative in conjunction with IT Asset Management services. To accomplish this, Team AveningTech will provide purchasing and receiving support for items such as approved design IT projects, software, connectivity services, biometric-related solutions, digital cameras, electro-optical devices, and other items that support the mission. To achieve best value, we will submit a written request for authorization to purchase with three (3) quotes (or a sole source justification/statement if it is a direct purchase), and we will utilize in-country vendors to the maximum extent practicable to provide support at the best cost. If an in-country vendor does not represent the best cost to the Government, Team AveningTech will locate the best vendor. As part of our asset management and GFE SOPs, we will be responsible for proper receipt, handling, storage, and accountability of items ordered under this contract until they are fully installed and operating according to system requirements.

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

Our team will provide regional oversight and management of Bilateral-Telecommunication and Networks infrastructure. 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-JPN (Japan-Bilateral Joint Network)​ and CENTRIXS-KOR (Korea-Bilateral Joint Network)​ on our PACAF SIPRNet contract. Our Army 403rd AFSB contract includes support of CENTRXIS-K network and exercise support with US Forces Korea (USFK)

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.

Since 2013, AveningTech has been a subcontractor to Leidos providing engineering and technical services support to PACAF/Joint bases across the Pacific theater. Our senior engineers sustain TS/SCI, Secret (including coalition systems/networks), and NIPRNet systems for ISR units at all PACAF bases. We provide engineering and technical support for the maintenance, sustainment, integration, and enhancement of the current Unit Level/Unit Command and Control (UL/UC2) Intelligence systems and any other Command, Control, Communications, Computers, and Intelligence, Surveillance, Reconnaissance (C4ISR) application/systems interfacing with PACAF ISR and other ISR systems/applications. We provide technical assistance to correct hardware/software discrepancies for PACAF-managed imagery systems and provide support to local and/or HQ PACAF and/other ISR Working and Steering Groups.

We provide hardware/software maintenance, system, security functions (including ISSO and CRO support), fault and problem isolation and resolution, and user support for ISR or other intelligence supporting units. Our team possesses extensive Common Operational Picture (COP) management experience. We provide installation and administrative support to GCCS-J and GCCS-I3 servers, clients and I3 Database and Applications Server instances. We installed GCCS-J v4.1.1 for 56 ACOMS to facilitate AOC GCCS involvement in Terminal Fury Exercises. We operate as the primary message sender and message traffic archiver for VAQ 142 using Defense Messaging System (DMS) and DMDS profiler. Additionally, we provide engineering solutions for Radiant Mercury and GCCS generated message traffic and networking solutions using CENTRIXS, BISON and Stoneghost and brief COCOMs and BILAT organizations on traffic flow and release-ability issues.

# Staffing Plan

For this effort, we have identified qualified and available candidates for each proposed position. Complete, detailed (redacted) resumes are provided as an appendix. Every proposed candidate has committed to working on this project if the AveningTech team is the successful bidder. Additionally, every candidate proposed has given express permission for the use of his/her resume in this proposal.

[Insert MS Word matrix of positions + locations, names/roles]

***Surge Support*** — Team AveningTech maintains bench support at the corporate level for areas that may be required by the government for surge support. We are able to draw on personnel from others contacts on an as-needed basis, should the situation arise where cleared, experienced personnel are needed to back-fill under emergency conditions. Team AveningTech will utilize the intake process to capture requirements identified by government stakeholders on potential upcoming activities that might stress the staffing resources. We will use this to assess the need for surge support and scope levels of effort based on low, medium, and high workloads. Within this process we will work with the client in augmenting resources, and identify funding for surge integration to alleviate costs while maintaining mission integrity during times of duress. Consider how Team AveningTech stands out: we implement a personnel process, “talent pipelining,” in which we identify candidates based on our expectation of potential future requirements. Team AveningTech then evaluates, with an often sponsor for clearance, to mentor and provide training materials to prepare the candidate for certification testing. We reimburse test fees and pre-qualify them. In this way, we’re able to draw from our database to select a candidate who is ready to start work with an average of two weeks’ notice.

***Recruiting and Retention*** — The processes we use to identify and retain key personnel are components of our PMO standard operating procedures (SOP). AveningTech continuously performs active recruiting to identify highly qualified and experienced personnel to support customer requirements. We maintain an extensive database of qualified candidates that we pre-qualify to support emerging hiring needs, and we offer a generous employee referral program, which draws qualified, like-minded and highly skilled individuals for employment consideration.

AveningTech uses various sourcing methods to draw qualified and diverse applicants, such as employee referrals, subscription services including Clearancejobs.com and, when necessary, the services of external recruiters. We partner with local colleges and universities and participate in job/hiring/career fairs — including those at Kapiolani Community College in Honolulu. We have access to an enormous pool of qualified and experienced veterans and military spouses worldwide as a partner in the Office of the Secretary of Defense Military Spouse Employment Partnership (MSEP). We are also associated with the White House Joining Forces Program and the US Chamber of Commerce Hiring Our Heroes Program and connect directly with veterans and military spouses seeking employment.

Access to this wealth of talent enhances our ability to ensure that positions are filled in a timely manner, reduces the time it takes to replace personnel, and extends our reach to areas in proximity to our client locations. When losing an employee and faced with the need to fill a vacancy on short notice, AveningTech targets a two-week maximum for backfilling the position. We have historically been able to meet this target timeframe in most cases and have had measurable success filling positions in the INDOPACOM region, including Hawaii, Guam, Japan, South Korea and Alaska.

Employee referrals are an important part of our process not only because our employees can attest to the capabilities and work ethics of the individuals they refer, but because referrals are a testament to the satisfaction felt by current AveningTech employees. We also receive frequent referrals from our customers and prime contractors due in part to our low turn-over rates and high levels of employee satisfaction reflected in our team's performance. AveningTech tailors the hiring for each effort to the specific needs of the contract or task order.

One result of AveningTech’s history of providing technical support to various Government agencies is our ability to properly vet candidates for proficiency, personality, and where they best fit in the organization. As a general practice, AveningTech tailors the hiring for each effort to the specific needs of the contract or task order. Therefore, our hiring approach includes tailoring the job descriptions, applications, interviews, follow-ups, and post-hire training appropriately for the specific skills and experience required for each position. Specifically, our job descriptions for each position contain tasking descriptions, certifications, education levels, and years of experience as explicitly called forth in the performance work statement. Our hiring and personnel placement reflect the diverse nature of the requirements within the PWS and the broad range of skills required to accomplish the tasking.

We provide our employees paid time off, including three weeks of vacation and 10 paid Federal holidays; medical, dental, vision, short- and long-term disability, life insurance, flexible spending, and retirement benefits that are commensurate with those provided by Fortune 500 companies. We are a military spouse and military veteran friendly company, tapping into the tens of thousands of un- and under-employed candidates attached to the military. We rely on our employees to deliver the highest caliber of support services to our clients and take every opportunity to catch them “doing something right.” We provide recognition and rewards to employees for superior performance, and those who consistently ensure that their clients are delighted with their support.

During initial on-boarding and throughout employment with AveningTech, supervisors and managers meet with employees to discuss career progression and advancement and develop strategies that include achievement of additional and higher-level certifications. Working with each employee, we determine their professional objectives, and make recommendations for education, training and certification testing required to achieve their goals. Security Considerations

In order to provide AveningTech’s customers with the highest level of assurance and confidence in our Security Program, we meticulously manage every aspect of our corporate security practices and processes. The processes and procedures detailed in the following paragraphs will be applied to all PWS and Task Order requirements.

We begin by ensuring we have a clear understanding of the security requirements of each individual Task Order as well as the general security requirements of the contract. For our work with the Department of Defense we utilize contractual guidance from the Form DD Form 254, Contract Security Classification Specification, where we obtain information about the highest level of classification of the work to be performed, location(s) of where the work will be performed, access requirements and security guidance/information. We understand that individual Task Orders may include DD Form 254, if required. Protection of classified information is our top priority.

The government interfaces with our PM for all personnel management issues — performance, shortfalls in staffing, replacements (temporary for absences, new hires for vacancies). Our PM works in the AveningTech portal to resolve employee issues regarding benefits, training, and labor laws. The HR department is part of our PMO. The PM will be interacting with the PMO. The PM will engage our recruiters to fill open positions rapidly when necessary. Our HR and recruiting teams use an online tool and our applicant tracking system (CATS) to organize and streamline our recruiting process and help to evaluate, screen, and schedule interviews with our PM and leads. Our PM will work with our Facility Security Officer (FSO), who uses Security Control (Sec-Con), a security management tool, to manage notifications, scheduling, submission, and management of the security clearances across our contracts, ensuring 100% compliance with security requirements.

Sec-Con offers built-in workflows to automate and track annual training/briefings, classified visits, foreign travel, new hire on-boarding, terminations, new contract awards, clearance upgrades/downgrades, and Incident reporting. Sec-Con provides AveningTech employees with a secure self-service portal in order to quickly and privately report insider threats and respond to action items through direct email notifications. Sec-Con employs a layered system of security mechanisms to provide the highest level of protection for data, including end-to-end encryption, two-factor authentication, and full audit of every user interaction with the system. Independent security assessments are routinely conducted against the Sec-Con software to make sure it is defending against evolving security risks. We have invested in these management tools and processes to eliminate manual, time consuming, and costly tasks. These tools and processes also allow us to optimize our personnel more efficiently, enabling better projections, and define business processes — all benefits that Government will derive from hiring AveningTech.

***Request for Clearances*** — DISS also allows us to enter a previously un-cleared employee into the e-QIP system to request a determination for eligibility to access classified information and systems. Our facility security staff also has experience using the Office of Personnel Management’s OPMIS Secure Portal (NP2) to access the e-QIP site and initiate an e-QIP application for an employee and if they did not possess any clearance eligibility, we would begin the process of requesting access to CNFJ/CNRJ facilities in accordance with CNFJ/CNRJ requirements.

***Management of Clearances*** — At present, AveningTech manages the security clearance/eligibility for over 75 employees. Our primary tool in administering their accounts is the Defense Manpower Data Center’s (DMDC’s) Defense Information Security System (DISS). DISS allows us to see current security information on each employee, manage visit requests and determine when their next periodic review may be due.

We ensure that AveningTech Team members understand their personal responsibility to report to the applicable Security Office any anticipated foreign travel, any changes in marital status or room/house mates, outside employment and any court cases as listed in the RFP. These reports will minimize the possibility that such events and occurrences will have a negative influence on their ability to safeguard classified information. AveningTech acknowledges and accepts that our assigned personnel may be required to undergo a counterintelligence-focused polygraph examination at any time and without notice.

Personnel who have been granted eligibility to work at CNFJ/CNRJ facilities will also be subject to the Continuous Evaluation Program (CEP) to ensure high standards of conduct are maintained and that questionable conduct or activities are promptly reported for adjudicative assessment. Soon, an automated records check monitoring system will be in place to cover the gap between initial investigation and periodic review.

All AveningTech Team personnel who will perform on any awarded Task Orders will be citizens of the United States and they shall meet the U.S. residency requirements identified in the RFP. They will also execute non-disclosure agreements for all information they may obtain while at any CNFJ/CNRJ worksite or at any AveningTech site that is dedicated to performing work for any awarded Task Order. The conditions upon which such a Warrantless Search may take place will be fully explained to employees prior to them being allowed access to any FBI or DOJ facility. The DD 1001 forms will be forwarded to the COR for retention during contract performance and two years thereafter. AveningTech understands the CNFJ/CNRJ requirements for both escorted and unescorted access to CNFJ/CNRJ facilities and will ensure the proper forms are completed and submitted in a timely manner to the COR for escorted access, or to the identified Chief Security Officer for unescorted access requests.

***Training*** — Team AveningTech team leaders will evaluate each team member performance and provide constructive guidance for improvement. In any situation where performance is unacceptable, our PM will provide assistance in training and mentoring those personnel. The team member’s progress will be reviewed during weekly leadership performance status meetings. If objectives are not met, further disciplinary actions are available, including dismissal. The team’s PM will be responsible for coordinating, planning and working with our human resources team to secure highly qualified resources needed to achieve all assigned task orders and/or project goals. Our PM will develop an Employee Development Evaluation Plan (EDEP) that defines individual performance and improvement progress objectives for review. Our team will provide formal and informal training to users and briefings to Government on current initiatives or other areas, as requested. Our IT personnel have in-depth experience in providing training to users both in person and remotely, via web-based video collaboration.

The culture of an organization is established by many factors, such as the ethical examples of behavior displayed by owners and senior managers, the work environment created through mutual trust and courtesy, and the information and education offered to employees of the organization. For decades, the AveningTech senior management team has devoted their efforts to supporting and defending the freedoms we enjoy today in the United States. That service has instilled in the company a culture of doing things right the first time, striving to improve our skills and abilities at every opportunity, and supporting each other to get the job done.

The introduction of a new employee to the AveningTech culture begins with their reading and acknowledgement of the AveningTech Employee Handbook. Here they learn of the company’s administrative processes and company policies. Many of these topics are common to all companies in the United States and their inclusion is a matter of regulation compliance.

As such, all our work in the management and technology fields requires us to protect the government’s classified information and material as we perform our services. To help a new employee quickly get up to speed on how to accomplish this critical security task, and to reinforce this behavior in our veteran employees — we require that they complete both initial and annual security training. Our new employees come to AveningTech with a diverse range of knowledge and experience. In order to either create or build upon their knowledge of Security fundamentals, we include the multiple general topics in their initial security briefing, the purpose being, to have them understand National and Customer-specific security policies to counter threats. Our goal is that they always maintain operational awareness at all times, whether at work or in their personal lives. The Annual Security Briefing is intended to reinforce the security elements and safeguards introduced in their initial security brief and to remind employees of their on-going security responsibilities.

Throughout the year, AveningTech’s Facility Security Officer conducts periodic training, and disseminates security-related information in the form of periodic e-mails, distribution of security brochures and hosting security teleconferences with key management and supervisors. The FSO Toolkit on the Center for Development of Security Excellence (CDSE) website offers shareable information/brochures on relevant topics.

**OCCI Mitigation Plan**

Team AveningTech has conducted a thorough audit of existing contracts, including personnel potential involved in this effort, and has found no conflict of interest, thus OCCI does not exist, per IAW DISA Special Contract Requirement H1. We have found no Organizational Conflict of Interest (OCI) exists because no persons are unable or potentially unable to render impartial assistance or advice to the Government. All our team members and proposed staff show objectivity in performing contract work, and therefore are not otherwise impaired, as there are no competing professional or personal interests found in our audit.

Team AveningTech personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. Team AveningTech will notify the Contracting Officer or Contracting Officer Representative immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and will promptly submit a plan to the Contracting Officer to avoid or mitigate any such OCI. Team AveningTech’s mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting Team AveningTech from participation in subsequent contracted requirements which may be affected by the OCI.

# Transition

***Transition-In*** — AveningTech understands the success of this program relies on an effective contract transition — in fact, contract transition is one of the most critical phases in the life of a contract. A transition that goes well sets the stage for good contractor/Government relations and smooth performance throughout the performance period. A transition that goes badly undermines relationships and confidence in the new contract team when cooperation between the Government and new contractor is most critical. It can take months to recover performance to acceptable levels.

Upon notice of award and before the start date — and non-billable to the government — we will initiate a pre-start-up phase so that the day of contract start will correspond with the start date of any new hires we are making to fill those inevitable empty slots. We understand that the support required cannot be allowed to degrade as a result of contract transition. We also understand that the best contract transitions are cooperative efforts between the customer and new contractor. All parties suffer when it goes badly, but most importantly, the mission suffers, an unacceptable situation. We will deliver a final Transition-In Plan no later than 5 business days after program kickoff.

While we have identified personnel to fill our entire anticipated level of effort, we believe the best approach to avoid disruption in service is to retain the incumbent staff, at least initially, and then subsequently work with the customer and the personnel to verify that they are indeed the best fit for each position. Over time, we may propose replacing personnel, with government concurrence, with our previously identified candidates, or we may recruit candidates with other skills and capabilities if necessary.

Recruiting and transitioning incumbent staff will ensure continuity of operations and minimize risk of degradation of service. We have conducted similar transitions in the past successfully. As the prime contractor supporting US Coast Guard TISCOM, we received notice of award on a Thursday evening, and had all 15 incumbent staff, including subcontractors, on site and ready to work the following Monday morning. On a recent contract awarded by the Marine Corps, we received notification of award on a Wednesday, and had 5 of the 6 key personnel on site and ready to work on the following Monday morning. As a small business, we are unencumbered by needless bureaucracy, and can execute background checks, clearance verifications, employment applications, offer letters, visit requests, and subcontracts seamlessly and rapidly. We work within the time allocated.

We have identified fully qualified, cleared and certified candidates for all positions as defined in the RFP. Resumes detailing their skills and experience and copies of required certifications are included.

While we are prepared to assign our proposed key personnel for every position on this contract, our expectation is that the Government may wish to retain some, if not all, of the incumbent staff. If that is the case, we intend to offer qualified and interested incumbent personnel first right of refusal, and retain them in their current positions with government concurrence.

We recognize that there are advantages and disadvantages of employing incumbent contractor personnel; incumbent personnel bring specific knowledge and firsthand experience that can make an important contribution to a seamless transition, but they can also be too tied to current practices and unwilling to make the necessary changes to improve contract performance.

Our stated strategy is to hire all incumbent staff — because that’s the most effective way to avoid disruption and ensure a smooth transition; however, in order to ensure we will satisfy customer expectations, we will carefully evaluate personnel to determine if all incumbent personnel are effective, assigned to the correct positions, and performing in accordance with expectations and requirements. At that point, we will start replacing non-performers with our previously identified personnel or propose new candidates (with customer approval). With the insight our teammate Leidos offers based on their prior history of supporting this organization, as well as their global reach, the government will get additional recruiting and staffing “bang for the buck.”

We recognize that a successful transition relies upon close collaboration with any out-going incumbent (if it exists), coupled with dedicated resources working towards a well-defined set of milestones. Short transition-in periods pose risks that need to be mitigated through close collaboration with all parties involved. The coordination, collaboration and cooperation from any outgoing contractor and the customer will be critical in ensuring the proper turnover of important project documentation, artifacts and process and procedures contributing to achieving operational readiness.

Our Transition Management Plan addresses all aspects of technical and cultural transition, and places emphasis on service continuity by minimizing the impact to operations. The main objective of the Transition Plan is to support project start-up and execution, and address change management and transformation with minimal impact on the client organization and ongoing efforts.

Phased Approach to Transition. Ordinarily beginning with Pre-Transition, through Transition Execution, and into Post-Transition, our phased approach addresses critical transition elements, including risk management, quality and performance management, organizational change management, communication, staffing, resource allocation, knowledge transfer and training. Ultimately, the objective is assimilation of operations, equipment and technology. These elements are integrated with our established quality management practices, ensuring our team will operate efficiently and effectively while obtaining the necessary knowledge transfer and appropriate staff conversion.

Our phased approach to transition relies on solid leadership by a committed and experienced transition team interfacing with the customer, and our application of proven practices fine-tuned through experience with similar transitions within the DoD environment. This approach will provide the client with the assurance of full commencement of services upon transition-in. Due to the requirement for a one-week transition, these activities will be abbreviated and compressed, but will still occur.

For each specific effort, our transition team works with the client to prepare a detailed schedule with milestones to ensure that we address every aspect of the project and comply with the client’s schedule for final handoff. We will schedule and conduct daily transition status meetings and provide a transition status report that includes clearly identified transition risks, issues and mitigation strategies. We will address the transition of personnel, processes, documentation, tools and technology to ensure that we have the tools and processes in place to complete necessary actions, and we will rely on open and constant communication to avoid any surprises during the course of the transition period.