Performance Work Statement (PWS)
Enterprise Cloud and Network Operations, and Management Services

Table of Contents

1.0 Introduction

1.1 Background:

The Navy has transitioned from an on-premise IL5 architecture to a cloud centric, zero trust architecture. Contractor support will include the operations and management, sustainment, and support for Cloud Environments and Services, including the current Azure Impact Level (IL) 4/5 security environment and Intune Management of Nautilus Endpoints.

Similarly, the Navy is transitioning the current on-premise classified architecture to a cloud centric, zero trust, IL6 architecture that enables secure access to Navy Cloud Services and its open and flexible cloud computing platform. The initiatives are aimed at bolstering Cloud Computing productivity services and network services while improving resiliency in the unclassified (IL5) and classified (IL6) environments across the Continental United States (CONUS) and outside CONUS (OCONUS). IL6 is reserved for storing and processing information classified up to the SECRET level, which pertains to classified information that, if compromised, could pose serious damage to national security interests. Efforts will include maximizing security and availability, while leveraging cloud efficiencies that include Artificial Intelligence and Machine Learning (AI/ML). Contractor support will augment the government workforce, in some cases on a 24x7 basis, while standing up a classified IL6 cloud environment, implementing and executing IT service management (ITSM) processes, maximizing efficiencies across both tenants, and delivering weekly status reports depicting network health and user impact. Contractor support will include sustaining the cloud security environment, and augmenting the management, sustainment, and establish cloud support model for the enterprise cloud architectures and future cloud services. The enterprise architectures are designed to support robust authentication, device hardening, and the reduction of the overall attack surface; improvements shall enhance capabilities to detect and quickly respond to adversarial activities. The implementation of IL5 and IL6 cloud services are instrumental in elevating the Navy's cybersecurity posture and advancing all concepts demanded in a Zero trust model. Furthermore, Microsoft Azure expertise is sought-after, with cloud experience desired with commercial cloud service providers (CSPs) such as but not limited to Amazon Web Services (AWS) and Google Cloud Platform (GCP), to facilitate expanding the existing Flank Speed (FS) infrastructure, including integrating with enterprise identity services, such as Naval Identity Services (NIS), the execution of design refinements, the deployment of additional advanced security features through automation, and the incorporation of new collaboration functionalities. These capabilities are essential to enhancing zero trust principles while further improving capabilities that include Hyper Converged (HCI) stacks that deliver enhanced computing power and more adaptable access to data and services hosted at the edge.

This PWS specifically covers Enterprise Cloud Services, Operations and Maintenance (O&M) for IL5 and IL6. While the primary operating platform will be hosted on Microsoft’s Azure, contractor support is expected to extend across other cloud services such as AWS, Google, and Oracle.

1.2 Purpose

The purpose of this PWS is to define requirements for the operations, sustainment, management, and defense of the Government's enterprise cloud and network ecosystem, with primary emphasis on 24x7 service operations. This PWS provides performance-based requirements to ensure confidentiality, availability, performance, compliance, and security for Microsoft Azure, Microsoft 365, Intune-managed endpoints, SD-WAN, and other CSP environments, while remaining cloud-agnostic to support multi-cloud operations.

1.3 Objective:

The objective is to procure a non-personal services contract to aid the government in various efforts, including Service Strategy, Service Design, Service Operations, Service Transition, and Continual Service Improvements across the cloud tenant. Contractor support must include, but not limited to architectural design, process development, network and service monitoring, sustainment, implementation, incident resolution, operations and maintenance of advanced security automation and collaboration features. These capabilities are essential to facilitate maximum access to Microsoft Azure Cloud services in a rapidly evolving operational networking environment, which will also extend to support AWS and Google services and Naval Exchange Point (NXP) Integration. Enterprise services and network access to the maximum extent feasible is crucial for users operating from any site utilizing Department of Defense (DoD) networks and shall align with the guidance as outlined in USCYBERCOM PLANORD 20-0042. Additionally, contractor services are required to deliver ongoing support for enterprise account management (i.e., e-Discovery, Records Management, Litigation Hold, CAPSTONE, etc.), and the migration of NXP network components, along with all associated support activities. This framework, founded on Azure identity and security services, will enable maximum access and secure convergence of both IL5 and IL6 environments that span across the Navy Enterprise Network (NEN) and the Department of Defense Information Network-Navy (DODIN-N). The totality of all efforts are crucial to broadening cloud capabilities, maximizing resiliency, and implementing state-of-the art technical advances using AI/ML; all work is intended to fully support future application integration as part of the broader Navy cloud migration strategy.

1.4 Scope

The scope of work encompasses the management of operational data, systems, and applications spanning several Impact Levels (IL) of information management, including IL 4, 5, 6, network transport, and Hyper-converged infrastructure (HCI) Stacks while addressing all use cases involving Controlled Unclassified Information (CUI), Classified Information, and Navy Nuclear Propulsion Information (NNPI). For direct contractor support within the IL6 environment, access to classified information at government facilities is required for all support staff. The ongoing implementation of an architecture that supports cloud services and the maturation of zero trust principles represent a significant transformation for both the Navy and the broader DoD. This transformation will demand substantial efforts, including the development or update of security policies, the re-engineering of systems, and the retraining of personnel to effectively operate, maintain, and secure the IL5/IL6 Azure Cloud environments. Furthermore, the Navy will continue to maximize the utilization of new collaboration and productivity features that require

meticulous planning, engineering, configuration, and change management. The Navy's strategy also includes migrating additional excepted networks and new applications into the IL5/IL6 Cloud architecture, to include Multi-Tenant Organizations (MTO). Architecture improvements include implementing enterprise cloud solutions that include installing Azure HCI Stacks that will effectively bring cloud services closer to end-users. This shift aligns with network resiliency and the Navy's objectives to enable an enhanced teleworking environment while concurrently reducing data center footprints and embracing modern cybersecurity principles, such as zero trust.

The ongoing development of the enterprise Azure cloud framework is crucial as it will facilitate centralized management and monitoring, improve network flexibility, and expedite the expansion of increased compute capacity and mission workloads where required. Additionally, this contract will support implementing a Records Management capability within the IL5/IL6 cloud tenant to meet Department of the Navy (DON) data retention, legal Litigation Hold, CAPSTONE requirements and e-Discovery search requests. The contractor shall provide enterprise IT support services, including but not limited to help desk, network operations, and cybersecurity.

The Contractor shall provide continuous operational, sustainment, management, and defense services for enterprise cloud and network systems. Services include administration of Microsoft ecosystem environments, endpoint management, SD-WAN operations, cybersecurity defense, ITSM functions, performance monitoring, reporting, incident resolution, and continual service improvement. The Contractor shall also support service design and strategy activities to ensure operational feasibility, maintainability, and alignment with evolving Government priorities.

2.0 References

a) DoD Directive 8140.01 CYBERSPACE WORKFORCE MANAGEMENT
b) SECNAV M-5239.2 Department of the Navy CYBERSPACE INFORMATION TECHNOLOGY AND CYBERSECURITY WORKFORCE MANAGEMENT AND QUALIFICATION MANUAL
c) Memorandum for Distribution: Subj: IT LEVEL DESIGNATION ON DD FORM 2875 SYSTEM AUTHORIZATION ACCESS REQUEST

3.0 Period of Performance:

The resultant Indefinite Delivery, Indefinite Quantity (IDIQ) contract will consist of the following five-year base ordering period and will contain FAR 52.217-8 – Option to Extend Services to allow for a six-month extension of the ordering period if circumstances necessitate the exercise of this option. The ordering periods are as follows:

Period of Performance	
One 5-Year Base Period	01 January 2027 – 31 December 2031
FAR 52.217-8	01 January 2032 – 30 June 2032

4.0 Place of Performance:

Work in accordance with this PWS shall be performed at:

(1) Primary Location: Naval Network Warfare Command, 112 Lake View Parkway, Suffolk, Virginia 23435.
(2) Secondary Locations at designated government facility.
(3) Remote and/or telework may be approved and authorized by the Government, should it be in their best interest

5.0 Performance Requirements:

The Contractor Support (CS) shall provide comprehensive **o**perations, incident resolution, sustainment, management, and defense services in accordance with DoD, DISA, and NIST guidance, while adhering to ITIL-based service operations best practices. CS is required to assist the Navy with worldwide acceleration and migration to Flank Speed, Nautilus and cloud service monitoring, network services and availability, and to sustain the continually evolving security and productivity features using zero trust secure technologies.

5.1 Cloud and Tenant Operations

The Contractor shall:

5.1.1 Operate, maintain, and secure Department cloud tenants within Microsoft Azure or equivalent CSP environments accredited for IL5 and IL6 workloads, ensuring compliance with DoD cybersecurity, Security Technical Implementation Guides (STIGs), and Risk Management Framework (RMF) requirements.
5.1.2 Engineer and implement solutions enabling key service dependencies, including identity management, authentication, routing, and hybrid integrations across on-premise, cloud environments and HCI stack resources.
5.1.3 Identify, document, and recommend decoupling strategies for hybrid dependencies, including DNS, load balancing, proxy services, and directory synchronization.
5.1.4 Perform capacity planning and lifecycle management of cloud subscriptions, resource groups, and workloads to ensure optimal performance, scalability, and cost efficiency.
5.1.5 Implement monitoring and alerting using native tools (e.g. Azure Monitor, Log Analytics, Purview, Sentinel) or equivalent CSP monitoring platforms for proactive incident detection and remediation.
5.1.6 Develop and maintain Continuity of Operations (COOP) and Disaster Recovery (DR) plans for cloud tenant services updating as needed, reviewing annually; testing failover and recovery plans and procedures annually at a minimum.
5.1.7 Manage Role-Based Access Control (RBAC), Privileged Identity Management (PIM), and audit administrative access logs for compliance and least-privilege enforcement.
5.1.8 Implement and manage governance controls such as Azure Policy, Blueprints, and tagging or equivalent CSP policy enforcement to standardize configuration and compliance.
5.1.9 Maintain cost management dashboards, resource tagging, and utilization reports to support

Government oversight and financial transparency.
5.1.10 Support cloud architecture development and configuration design aligned with Zero Trust principles and DODIN connectivity requirements.
5.1.11 Coordinate with Government and vendor stakeholders to ensure configurations comply with DoD Cloud SRG and FedRAMP security baselines.
5.1.12 Operate and maintain edge or hybrid HCI stacks (e.g. Azure Stack or equivalent CSP hybrid platform) at Government and/or Commercial data centers to optimize performance and ensure operational continuity.

5.2 Network and SD-WAN Management

The Contractor shall:

5.2.1 Operate, monitor, and maintain network infrastructure supporting cloud and Microsoft 365 connectivity including routers, firewalls, SD-WAN appliances (i.e. NXP), and encryption devices.
5.2.2 Perform end-to-end SD-WAN management across CONUS and OCONUS locations, AFLOAT, maintaining configuration synchronization and connectivity compliance.
5.2.3 Manage firmware updates, configuration backups, and rollback plans for SD-WAN devices and controllers.
5.2.4 Monitor network performance metrics including latency, jitter, and throughput, maintaining service levels in accordance with approved thresholds.
5.2.5 Manage routing policies, quality of service (QoS) parameters, and segmentation rules consistent with DoD transport security requirements.
5.2.6 Perform proactive diagnostics, analyze transport anomalies, and coordinate with DoD or vendor entities for resolution.
5.2.7 Comply with Network Configuration Management Plans and sustain a Configuration Management Database (CMDB) tracking all SD-WAN and network assets and configuration items.
5.2.8 Ensure all network configurations comply with encryption and cybersecurity standards defined by DISA and DoD CIO.
5.2.9 Manage network baselines, align with change control actions, and incident resolution activities within the approved ITSM system.

5.3 Cloud Tenant and Microsoft 365 Management

The Contractor shall:

5.3.1 Administer M365 and equivalent SaaS platforms to include but not limited to Exchange Online, SharePoint, OneDrive, Teams, Intune, and Virtual Desktop infrastructure.
5.3.2 Manage identity and access cloud directory services (i.e. Microsoft Azure Entra ID or equivalent Active Directory), ensuring synchronization with DoD Global Directory and DISA (i.e. Defense Enterprise Provisioning Online (DEPO), etc.) identity and entitlement provisioning processes.
5.3.3 Administer user and administrative accounts, roles, and access privileges according to

least-privilege principles.
5.3.4 Monitor and remediate synchronization, licensing, and access issues within the tenant environment.
5.3.5 Manage Conditional Access, Defender for Cloud Apps, and equivalent security policies, ensuring compliance documentation and testing validation are maintained.
5.3.6 Manage licensing allocation, reclamation, and forecasting for all Microsoft 365 or equivalent services.
5.3.7 Coordinate and validate feature rollouts, updates, and service changes; conduct impact assessments, and communicate release schedules to stakeholders.
5.3.8 Perform tenant-level health assessments, readiness checks, and service optimization to sustain operational reliability.
5.3.9 Ensure data retention, backup, and recovery processes meet DoD and NARA requirements for mission-critical workloads.
5.3.10 Manage hybrid integrations (Exchange Hybrid, AAD Connect, or equivalent) ensuring secure coexistence and continuity between on-premise and cloud environments.
5.3.11 Maintain governance over collaboration platforms, including SharePoint and Teams, ensuring appropriate permissions, structure, and lifecycle management.
5.3.12 Produce operational dashboards and reports on tenant availability, license utilization, and SLA performance.

5.4 Endpoint Management

The Contractor shall:

5.4.1 Operate and maintain endpoint management solutions (Microsoft Intune or equivalent) to enforce configuration baselines, compliance policies, and patch management.
5.4.2 Manage endpoint enrollment, provisioning, and retirement for all devices (Windows, iOS, Android, and other supported platforms).
5.4.3 Enforce device compliance policies for encryption, antivirus, OS version, and security posture.
5.4.4 Maintain endpoint groups, configuration profiles, and conditional access policies integrated with Azure AD or equivalent identity platform.
5.4.5 Integrate endpoint protection with Defender for Endpoint or equivalent, ensuring Zero Trust enforcement and continuous monitoring.
5.4.6 Monitor and respond to endpoint security alerts, remediating compliance drift within defined SLAs.
5.4.7 Maintain standard operating system images, application deployment packages, and automation scripts for consistent endpoint configuration.
5.4.8 Provide monthly reports detailing device compliance rates, patch status, and endpoint health metrics.

5.5 IT Service and Cloud Service Management

The Contractor shall:

5.5.1 Perform IT Service Management (ITSM) in accordance with DoDI 8440.01, ITIL, and the DESMF framework, including:

- Incident Management
- Problem Management
- Change Management
- Configuration Management
- Event Management
- Identity and Access Management
- Service Request Management
- Information Security Management
- Security Compliance

5.5.2 Integrate ITSM tools with CSP-native monitoring systems to support automated alerting, event correlation, and incident escalation.
5.5.3 Maintain ITSM artifacts including CMDB updates, change requests, problem records, and incident reports.
5.5.4 Develop and report SLAs, KPIs, and performance metrics for cloud and network operations.
5.5.5 Provide dashboards and analytics reflecting service health, availability, cost, and compliance posture.
5.5.6 Develop and maintain knowledge articles, standard operating procedures, work instructions, and other plans, procedures and lessons learned within a central knowledge repository.
5.5.7 Support RMF accreditation, compliance assessments, and cybersecurity audits for all operational environments.

5.6 Records Management, eDiscovery, and Compliance

The Contractor shall:

5.6.1 Execute Records Management processes to support search, retrieval, litigation hold, eDiscovery requests, and Capstone compliance in accordance with DoD policy.
5.6.2 Generate and distribute audit logs and compliance reports from Microsoft Purview or equivalent CSP compliance tools.
5.6.3 Create and manage eDiscovery cases, content searches, and disposition workflows.
5.6.4 Perform data disposition, destruction, or archival transfer to NARA per applicable policies.
5.6.5 Support electronic spillage response and execute containment, remediation, and reporting procedures.

5.7 Program, Security, Financial, Technical, and Documentation Management

The Contractor shall:

5.7.1 Provide program and project management for all deliverables and maintain alignment with Government objectives and mission outcomes.
5.7.2 Develop and submit monthly progress, risk, and financial reports in Government-approved formats.
5.7.3 Maintain TTPs, SOPs, and process documentation across all service areas, updating them as environments or policies evolve.
5.7.4 Develop and maintain COOP documentation, system design packages, and operational diagrams for cloud and network environments.
5.7.5 Provide technical briefings, reports, and executive updates summarizing current performance, issues, and improvement initiatives.
5.7.6 Maintain authoritative documentation repositories accessible to Government-designated personnel.
5.7.7 Provide financial analysis and budget reporting support.

6.0 Security Requirements:

6.1 Security: The contractor shall be responsible for adhering to all Department of Defense (DOD), Department of the Navy (DON) and Command instructions, guidance, orders, directives, and supplements relative to performing tasks set forth in this PWS. The contractor and its contract service providers shall not disclose and must safeguard procurement sensitive information, operationally sensitive data, computer systems and data, Privacy Act data, law enforcement data, litigation related data, and Government personnel work products that are obtained or generated in the performance of this contract. This includes dissemination of protocols and papers not generally available through public literature. Neither the contractor nor any of its contract service providers shall disclose or cause to disseminate any information concerning operations of military activities. Such action(s) could result in breach of the contract and possible legal actions.

Access will be granted to Government facilities as required in support of the tasking. Contractor personnel performing work under this contract must meet all requirements for gaining access to US Government installations. The contractor shall conform to all DoD, DON, and local (base/installation) security instructions; refer to Contractor Unclassified and Classified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information.

The scope of work requires all contractor personnel to hold a security clearance. For general administrative work, personnel must hold a Secret clearance, which requires a Tier 3 (T3) investigation. For personnel with domain/root level administrator accounts, a Top Secret clearance, which requires a Tier 5 (T5) investigation (or equivalent), is mandatory. Contractor personnel must possess the appropriate final or interim clearance by the first day of the period of performance. Where annotated, certain positions may require a Secret clearance that is supported by a Single Scope Background Investigation (SSBI)/Tier 5 investigation. An Interim Top Secret clearance, granted upon the initiation of an SSBI, is acceptable pending final adjudication.

All work is to be performed in accordance with DOD and Navy Operations Security (OPSEC) requirements and in accordance with the DD Form 254 and all attachments.

The contractor shall comply with all applicable federal, state, and local laws and ensure performance is secure while protecting material, equipment, and supplies from damage and loss. Government security personnel shall have the express right to inspect for security violations at any time during the term of the contract.

The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment and materials shall be secured.

The Common Access Card (CAC) card serves as the primary method of identification for the contractor employees, as well as providing the basis of Public Key Infrastructure (PKI) access to the Navy/Marine Corps Intranet (NMCI), the NCDOC Excepted network, and numerous Navy web sites, which may also require PKI access. The COR shall assist in providing the contractor the appropriate documentation for obtaining CACs. The contractor shall be responsible for obtaining any Government issued identification cards from former employees or employees whose access has been terminated and to turn those items over to the COR upon termination of employment or access.

Contract personnel shall wear a badge that clearly identifies them as a contractor employee. The badge will be issued by the COR, via the Special Security Office (SSO), and will contain a personal picture, name of employee, and contractor's name. Badges shall be worn on the outer garment, above the waist, in full view at all times, attached to the outer shirt or jacket pocket by a button or clip or worn around the neck secured by an appropriate identification card lanyard.

6.2 Privacy Act Compliance: The contractors may be in contact with data and information subject to the Privacy Act of 1974 (Title 5 of the U.S. Code Section 552a). The contractors shall ensure that its employees assigned to this effort understand and adhere to the requirements of the Privacy Act and to Department of Defense and Department of the Navy regulations that implement the Privacy Act. Department of Navy policy and procedures implementing the Privacy Act are detailed in SECNAVINST 5211.5E (Department of the Navy (DON) Privacy Act (PA) Program). The contractors shall identify and safeguard data, information and reports accordingly. In addition, the contractor shall ensure that contractor employees assigned to the contract are trained on properly identifying and handling data and information subject to the Privacy Act prior to commencing work.

6.3 Government Furnished Equipment (GFE): GFE will be provided to contractor employees as needed to complete the tasks set forth in this performance work statement. Access to classified information must be granted in accordance with the terms and conditions contained in DOD Manual 5220.22-M and DD Form 254 (Contract Security Classification Specification). The contractor shall comply with all current information assurance awareness, information security policies, procedures, and statutes applicable to DOD information technology; including DOD Instruction 8500.01 on Cyber Security.

7.0 DOD 8140 CYBER SECURITY WORKFORCE (CSWF) REQUIREMENTS:

The contractor shall ensure employees have all required certifications/licenses (current and valid) for each applicable occupation category before commencement of work. Contractor must meet this qualification upon first day of employment.

Procedures surrounding the qualification of the DON Cyberspace IT/Cybersecurity Workforce must be in accordance with DoD Directive 8140.01. The SECNAV M-5239.2 establishes mandatory procedures for the uniform identification, management, and qualification of the Cyberspace IT/Cybersecurity Workforce (Cyber IT/CSWF). The contractor must demonstrate upon request by the COR that all Cyber IT/CSWF personnel have met and maintains the minimum qualification standards of their assigned Specialty Area and proficiency level throughout the duration of this contract. DON has identified appropriate training, education, and industry certification requirements along with proficiency demonstration in the lab or on the job. All contractor personnel are required to carry an approved certification for their particular job classification.

Any full or part-time contractor personnel, with privileged access to a DoD information system, performing Cyber Security (information assurance) functions, regardless of job or occupational series, must meet the requirements associated with the CSWF specialty area outlined in the position description to maintain employment as part of this contracting effort. Additionally, all contractors must participate in a continuous learning program as described in SECNAVINST 1543.2. A minimum of 20 hours of Cyber IT/CSWF related continuous learning must be annually documented and available to NNWC's CSWF Program Manager and/or COR. Additionally, all contractor personnel must provide proof that required annual maintenance fees are paid within seven (7) days of the due date.

All reporting contractor personnel must meet the CSWF requirements specified for their position immediately upon arrival.

8.0 GENERAL/ADMINISTRATIVE MATTERS:

The contractor shall only conduct business with designated government personnel listed as points of contact (POCs). Names of authorized personnel shall be provided to the contractor by the government COR, in writing, and updated as necessary throughout the contract period.

All inquiries, comments or complaints arising from any matter observed, experienced, or learned of as a result of or in connection with the performance of this contract, the resolution of which may require the dissemination of official information, shall be directed to the COR. The COR will forward inquiries, comments or complaints to the Contracting Officer (KO).

8.1 Staffing: The contractor shall provide a fully qualified workforce on the first day of contract performance.

All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed. Additionally, they must clearly indicate on email title blocks their company name and that they are contractor personnel.

8.2 Data Rights: It is the Government's intent to retain unlimited rights to all software, documentation, and data first produced in performance of the task.

U.S. Government records, copies of original results and reports, verified original data, corrected data, and corrected supporting final reports are maintained by the contractor, but remain the property of the U.S. Government. These files/results must be surrendered to the COR immediately upon demand.

8.3 Contractor Quality Assurance: The contractor shall develop and maintain a Quality Assurance Plan (QA Plan) in order to ensure only qualified personnel, as defined in the position descriptions, are assigned to fulfill the requirements stated in this PWS. The contractor shall detail in its quality assurance plan how it intends to maintain personnel qualifications and ensure contract employees have up-to-date training and knowledge in their respective areas of endeavor.

This QA Plan shall detail the methodology to be used by the contractor to monitor and grade the performance of its personnel as they carry out the requirements of this PWS. The QA Plan shall address the contractor's courses of action to address under-performing employees.

8.4 Government Quality Assurance Surveillance: The Government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government must do in order to ensure that the contractor is performing in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

8.5 Complaints Lodged Against Contractor Personnel: In the event that a complaint is made regarding the conduct or ability of contractor personnel, the individual receiving the complaint will contact the COR. The COR will notify the contractor. The Contract Overarching Project Manager and COR will cooperate in investigating complaints made against contractor employees. If the results of the investigation prove the complaint(s) to be valid, the contractor shall have a maximum of three (3) working days to propose a corrective plan for resolving the matter and preventing future similar occurrences. This plan shall be submitted in writing to the Contracting Officer and COR. In the event that the Government deems the corrective plan insufficient for resolution of the problem, a written response to the contractor shall be provided within three (3) working days.

8.6 Office Space: Government will provide office space, desk, chair, and common office supplies. In addition to office space, each contract employees shall be provided with access to Government computers and telephones, but not cellular phones, for official use only. Under no circumstances will contractor-provided personal computers, electronic devices, or cellular phones be connected to the Navy/Marine Corps Intranet (NMCI). Contractor personnel shall comply with all DOD and Navy internet usage and cybersecurity policies.

8.7 Statement of Non-Personal Service: Contractor employees performing services under this contract will be controlled, directed, and supervised at all times by management personnel of the contractor. Contractor management shall ensure that employees properly comply with the performance work standards outlined in the PWS. Contractor employees shall perform their duties independently, under the supervision of, an appointed Government official. The tasks, duties, and responsibilities set forth in this contract shall not be interpreted or implemented in any manner that results in contractor employees creating or modifying Federal policy, obligating the appropriated funds of the United States Government, overseeing the work of Federal employees, providing direct personal services to Federal employees, or otherwise violating the prohibitions set forth in Parts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR) http://farsite.hill.af.mil/. The Government shall control access to the facilities and shall perform the inspection and acceptance of completed work.

8.8 Mandatory Training: Government has annual training requirements for the safety and security of personnel and data that will be required to be completed by all assigned contractors. This training will be provided by Government personnel, either in person or via computer, for completion during normal working hours. The COR will provide the annual required training list to the Company Program Manager on an annual basis, and completion will be tracked by the COR.

10.0 SUPPORT SERVICES/QUALIFICATIONS/DUTIES:

Position 1. Project Manager II (PM II):

DESCRIPTION:

These positions have been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 802, and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. Manages strategy, personnel, infrastructure, policy enforcement, emergency planning, security awareness, and/or other resources. Coordinate the efforts of subordinate SMEs including approval of and compliance with Tactics, Techniques and Procedures (TTPs) and Standard Operating Procedures (SOPs); coordinate with Naval Network Warfare Command (NNWC) teams to maximize effect of analysis of Flank Speed-generated data; and provide day to day leadership and guidance to all members of the Operation Flank Speed Effort. The contractor shall facilitate delivery of OFS Program Management tracking / artifacts / documentation to the COR or his / her designated representative.

QUALIFICATIONS REQUIRED:

- Clearance requirement is SECRET
- Experience managing 30+ people
- 12 years IT experience with MS365 Software as a Service offerings, cloud applications, and network management
- Extensive understanding of operating systems and networking
- Organizational skills
- Capable of managing multiple projects
- Great communication skills (oral and written)
- Azure Fundamentals Certification
- Microsoft 365 Fundamentals Certification
- Comprehensive understanding of cloud computing and networking
- Azure Firewall Knowledge
- Experience with Microsoft Office suite and PowerShell
- Experienced in the administration of Microsoft SharePoint

CONTRACTOR SHALL:

Provide administrative support for centralized preparation of all contract related deliverables, and ensure contractor deliverables are aligned with critical agency priorities.

Provide financial management support for centralized tracking, analysis and reporting all contract related funding, costs, and expenditures required the execution of this contract.

- Prepare monthly status/progress report for contract tasks
- Prepare monthly contract financial reports
- Prepare technical reports as required by specific projects
- Provide contract tracking deliverables to the COR monthly
- Liaison between contractor workforce and NNWC leadership for administrative purposes
- Ensure all contractor tasks are accomplished in a timely manner and that the proper support is being delivered
- Ensure product delivery is in alignment with intended government outcomes
- Deliver and maintain all TTPs/SOPs and exceptions assigned by government lead
- Coordinate and deliver additional tasking as assigned by OFS government leads; ensuring product delivery is in alignment with intended outcomes

Have knowledge to effectively oversee contractor workforce AND augment contractor workloads while performing the following functions:

- Managing Azure identities and governance
- Implementing and managing storage
- Monitoring and conducting back-up to Azure resources
- Configuring and managing virtual networking
- Be familiar with the hierarchal structure utilized in SharePoint sites hosted in Flank Speed
- Provide support for Teams Live Events as requested

- Monitor Microsoft 365 Admin Center for service-related incidents, outages, and feature releases
- Monitor Azure Information Protection data labels and controls
- Participate in various ITSM roles and activities (as required) including but not limited to change management, incident management and problem management
- Monitor, analyze and respond to alerts from M365 SaaS cloud operational and security tools and services
- Analyze SaaS cloud operational performance and trends, and support applications and systems on premise, in cloud, inclusive of network, server, and endpoints
- Deploy and manage virtual machines in Azure to support a large user base
- Provide technical support to the Enterprise Flank Speed Tier 2 service desk for troubleshooting issues as required
- Review and provide recommendations regarding group policy and end user software
- Provide recommendations regarding hierarchal management of SharePoint sites hosted in OFS

Position 2. Technical Writer (SME III):

DESCRIPTION:

The contractor shall perform quality reviews, rewrites, and editing of a wide-range of documentation throughout the command. Works with technical experts to develop, design, edit, all forms of documentation to include Standard Operating Procedures (SOPs), Process Guides, Instructions, Notices, Memorandums, Concept of Operations (CONOPS), and other written deliverables as requested.

QUALIFICATIONS REQUIRED:

- Clearance requirement is SECRET
- 3+ years IT experience
- Fluent spoken and expert written English language skills
- Experience in authoring executive level documentation written requirements, drafting Operating Procedures, delivering/documenting test results, etc.
- Expert level experience in Microsoft Word, and PowerPoint to include creating/applying styles, headers, footers, etc.
- Familiar with tracking changes and version control
- Experience with a Configuration Management tool (SharePoint) is preferred
- Robust attention to detail
- Strong organizational skills, with the ability to work on multiple projects with multiple deadlines
- Proven ability to collaborate and negotiate with multiple stakeholders to steer and document projects through the requirements phase, establish a consensus, and complete within established timeframe
- Be able to write for multiple audiences: project managers, subject matter experts, developers, system administrators, QA testers, technical support, end users, and executive

decision makers.
- Be able to write multiple documentation types, technical and non-technical: design specifications, technical requirements, installation procedures, system administration/management, test plans
- Working knowledge of the Information Technology Infrastructure Library (ITIL) Framework
- Working knowledge of government CIVPERs classification processes, as required to write evaluation statements for positions that will transition to CES

CONTRACTOR SHALL:

- Develop detailed technical and non-technical briefings, providing informational updates to chain of command in current and future development and implementation of measurements and data strategies
- Combine disparate materials into documents that flow logically and speak with one voice.
- Translate complex concepts and solutions into multiple types of documents (requirements, compliance, SOPS, test results, etc.)
- Draft documentation, user guides for all user levels, technical support and FAQs, as well as executive summaries
- Develop Standard Operating Procedures (SOPs), checklists, workflow process charts, forms, Points of Contact (POC) lists, and other documentation needed to support processes and related IA functions
- Create and maintain existing and potential data sources for local consumption; collaborate with data architect to ensure data sources availability
- Develop MS Power Point slides, MS Excel workbooks, and executive level word documents for review and forwarding to leadership
- Create and maintain existing and potential data sources for local consumption; collaborate with data architect to ensure data sources availability

Position 3. Conditional Access Policy Administrator:

DESCRIPTION:

These positions have been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 461 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. The contractor shall perform tasks associated with the development, testing, deployment, and documentation of Microsoft Azure Conditional Access and Microsoft Defender for Cloud Application policies.

QUALIFICATIONS REQUIRED:

- Clearance requirement is TOP SECRET
- 5+ years IT experience with significant experience with Microsoft Azure

- Azure Fundamentals Certification
- Azure Administrator Certification
- Understanding of cloud computing and networking
- Superior organizational skills
- Capable of managing multiple projects
- Great communication skills (oral and written)
- Familiar with tracking Access Requests and account provisioning
- Experience with Account and Access Management capabilities/tools
- Familiar with M365 SaaS Personas, and license types
- Strong attention to detail
- Working knowledge of the Information Technology Infrastructure Library (ITIL) Framework

CONTRACTOR SHALL:

- Maintain detailed documentation of conditional access policy, including archiving relevant configuration files to a centralized data repository
- Develop, document, test, and deploy Microsoft Azure conditional access policies.
- Develop, document, test, and deploy Microsoft Defender for Cloud Applications policies.
- Perform verification and validation that approved changes are made properly
- Perform account access provisioning and de-provisioning based on approved processes
- Evaluate policies to ensure compliance with DoD Tenant Configuration Guides
- Where development outpaces existing guidance, support development of DoD Tenant Configuration Guides with mission partners and DISA.
- Monitor Message Center for feature releases that have the potential to impact existing configuration, access roles and personas

Position 4. Azure Virtual Desktop System Administrator

DESCRIPTION:

This position has been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 461 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. Administers Navy Flank Speed Azure desktop environment server-based systems, security devices, distributed applications, network storage, and performs systems monitoring. Consults on network, application, and customer service issues to support computer systems' security and availability.

QUALIFICATIONS REQUIRED:

- Clearance requirement is TOP SECRET
- Comptia Sec +
- 5+ years IT experience with significant experience with Microsoft Azure
- Relevant experience as a Windows system administrator

- Understanding of cloud computing and networking
- Experience with PowerShell
- Knowledge of Microsoft Cloud Security and Data Governance Tools
- Superior organizational skills
- Capable of managing multiple projects
- Great communication skills (oral and written)
- Strong attention to detail
- Working knowledge of the Information Technology Infrastructure Library (ITIL) Framework

CONTRACTOR SHALL:

- Deploy and manage virtual machines in Azure to support a large user base
- Closely monitor session statistics to develop and refine usage metrics to inform provisioning additional resources or shutting down unused resources; assist in development of service optimization models
- Provide technical support to the Enterprise Flank Speed Tier 2 service desk for troubleshooting issues as required
- Manage Windows image to include group policy and end user software

Position 5. Cloud Service Support Administrator/Analyst:

DESCRIPTION:

These positions have been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 461 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. The contractor shall perform tasks associated with the administration of Microsoft 365 Software as a Service (SaaS) offerings, to include AZURE Virtual Desktop, Intune, Exchange Online, OneDrive, Teams, and SharePoint. Additionally, the contractor will perform administrative functions associated with Azure Information Protection/data labeling and control.

QUALIFICATIONS REQUIRED:

- Clearance requirement is TOP SECRET
- 3+ years IT experience Azure Cloud Administrator in an enterprise level cloud computing environment
- Azure Fundamentals Certification
- Microsoft 365 Fundamentals Certification
- Comprehensive understanding of cloud computing and networking
- Azure Firewall Knowledge
- Experience with Microsoft Office suite and PowerShell
- Experienced in the administration of Microsoft SharePoint
- Knowledge of Purview
- Basic experience with Power Platform

- Experience with Microsoft Cloud Security and Data Governance Tools
- Superior organizational skills
- Capable of managing multiple projects
- Great communication skills (oral and written)
- Strong attention to detail
- Working knowledge of the Information Technology Infrastructure Library (ITIL) Framework

CONTRACTOR SHALL:

- Perform administrative tasks associated with the management of Microsoft 365 SaaS offerings
- Manage Azure identities and governance
- Implement and manage storage
- Deploy and manage Azure compute resources
- Configure and manage virtual networking
- Monitor and back up Azure resources
- Configure and manage virtual networking
- Oversee the hierarchal management of SharePoint sites hosted in Flank Speed
- Manage tenant-wide configuration settings for Microsoft SaaS offerings
- Provide support for Teams Live Events as requested (e.g., conferencing/telephony support)
- Monitor Microsoft 365 Admin Center for service-related incidents, outages, and feature releases
- Manage Azure Information Protection data labels and controls
- Participate in various ITSM roles and activities (as required) including but not limited to; change management, incident management and problem management
- Monitor, analyze and respond to alerts from M365 SaaS cloud operational and security tools and services
- Perform M365 SaaS cloud service operations, analyze operational performance and trends, and support applications and systems on premise, and in cloud, inclusive of network, server, and endpoints
- Deploy and manage virtual machines in Azure to support a large user base
- Provide technical support to the Enterprise Flank Speed Tier 2 service desk for troubleshooting issues as required
- Manage Windows image to include group policy and end user software
- Oversee the hierarchal management of SharePoint sites hosted in Flank Speed
- Manage tenant-wide configuration settings for Microsoft SaaS offerings

Position 6. Cloud Service Support Engineer (SME II):

This position has been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 461 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. CONTACTOR will recommend configuration changes, test, operate, monitor, and manage network devices

including hardware, software, and operating systems that permit information sharing across the full spectrum of Navy Flank Speed Cloud Transport using all media. Supports the security of information and information systems.

QUALIFICATIONS REQUIRED:

- Clearance requirement is TOP SECRET
- 3+ years IT experience with significant experience with operational metrics correlation, reporting, and dash boarding in a Microsoft SaaS environment
- Familiarity with concepts of data integration and normalization
- Experience working in an IT environment in an operational capacity
- Ability to gather metrics and report on relevant findings
- Ability to use professional knowledge to collaborate with multiple competencies within the Navy
- Comprehensive understanding of SLAs/SLRs and service performance quality tools, processes, and procedures
- Technical understanding with ability to translate reports into mission capabilities
- Practical application of statistical, numerical and analytical principles and processes
- Relationship management and conflict resolution skills
- Proficiency in M365 and Microsoft Office applications including Word, Visio, Project, and PowerPoint
- Proficient to Master level Microsoft Excel and Access skills
- Excellent written and verbal communication skills
- Knowledge of Information Technology Service Management (ITSM) and ITIL Framework
- Knowledge of performance measurements and metrics methods and concepts
- Knowledge of Figures of Merit (FOM), Critical Success Factors (CSF) and Key Performance Indicators (KPI)
- Knowledge of pertinent Government laws and information technology regulations as well as applicable laws, policies, standards and guidance
- Knowledge of DoD requirements definition and how requirements drive KPPs, KSAs, SLAs and SLRs
- Knowledge of DoD and DON acquisition management principles, policies and procedures

CONTRACTOR SHALL:

- Leverage best practice BA/BI data correlation, aggregation and reporting in support of the Enterprise M365 SaaS capabilities
- Develop dashboards, reports, presentations and actionable recommendations and escalations related to M365 SaaS enterprise service performance and quality
- Identify performance measures or indicators of service performance, quality and compliance with SLAs/SLRs
- Develop/Deliver monthly performance reports on-time and on-quality

- Create Executive level dashboards to effectively communicate/socialize M365 SaaS performance to customer commands (CONUS & OCONUS)
- Facilitate ongoing assessments and reporting of overall conformance to and compliance with Critical Success Factors (CSFs) and Key Performance Indicators (KPIs) defined within the DoD Enterprise Service Management Framework (DESMF), DoDI 8440.01 Information Technology Service Management (ITSM), and COMNAVIFOR M-2620.2 Navy Process Reference Model where applicable
- Develop dashboards, reports, presentations and actionable recommendations and escalations related to Flank Speed Transport service performance and quality
- Routinely monitor circuit bandwidth capacity and make recommendations for bandwidth increases
- Identify transport anomalies and coordinate resolution with appropriate organizations
- Implement robust encryption protocols to protect data during transport. Proactively monitor vulnerabilities to transport services
- Conduct network diagnostics, performance optimization and incident resolution

Position 7. Cloud Application Administrator (SME II):

This position has been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 461 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. Administers Navy Flank Speed Cloud Applications environment server-based systems, security devices, distributed applications, network storage, and performs systems monitoring. Consults on network, application, and customer service issues to support computer systems' security and availability.

QUALIFICATIONS REQUIRED:

- Clearance requirement is TOP SECRET
- 7 - 10 years of experience as Azure Cloud Administrator in an enterprise level cloud computing environment
- Azure Fundamentals Certification
- Microsoft 365 Fundamentals Certification
- 3 years' experience working with RMF based Information Security Systems Engineer (ISSE) documentation
- Proficient in the application of Secure Technical Implementation Guides (STIG) on cloud-based systems
- Familiar with enterprise backup software and administration
- Familiar with enterprise storage administration and concepts
- Ability to work in team setting, as well as independently
- Self-starter: identify issues and create action plan for resolution
- Demonstrated initiative, flexibility and ability to concurrently manage multiple deadline-driven tasks and projects
- Excellent communication skills

CONTRACTOR SHALL:

- Provide Subject Matter Expert level support for desktops in Azure cloud computing environment
- Maintain systems patches
- Maintain systems security posture
- Implement STIGs
- Improve system administration productivity by authoring/updating relevant shell scripts
- Provide timely reports on projects status and other systems administration work, as required
- Aggregate custom detections and alerts into a cloud native SEIM
- Provide/perform on-the-job training of KQL for all assigned government and military analysts
- Provide/perform on-the-job training of Navy owned Microsoft products and capabilities for all assigned
- Assist in the development of a standardized cloud-based case management system

Position 8. Configuration Manager:

DESCRIPTION:

These positions have been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 461 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. The contractor shall perform tasks associated with the documentation and enforcement of technical baselines in support of change management, process and evaluate change requests, and maintain configuration control artifacts to support accreditation and monitoring in accordance with the DoD Risk Management Framework**.**

QUALIFICATIONS REQUIRED:

- Clearance requirement is TOP SECRET
- 5+ years IT experience
- Azure Fundamentals Certification
- Azure Administrator Certification
- Strong understanding of cloud computing and networking
- Superior organizational skills
- Capable of managing multiple projects
- Great communication skills (oral and written)
- Familiar with tracking enterprise changes and version control of assets and configuration items (CIs)
- Experience with Enterprise IT Configuration Management tools
- Experience with hybrid IT architectures across on premise and SaaS offerings
- Strong attention to detail
- Working knowledge of the Information Technology Infrastructure Library (ITIL) Framework

- Working knowledge of the DoD Risk Management Framework

CONTRACTOR SHALL:

- Assist in the development of the baseline E2E M365 SaaS architecture and configuration in hybrid environment
- Maintain detailed documentation of tenant configuration, including archiving relevant configuration files to a centralized data repository
- Assess planned changes for risk and impact across the hybrid environment
- Perform verification and validation that approved changes are successful and achieve expected outcomes
- Evaluate requested changes to ensure compliance with higher-level polices and directives
- Monitor Message Center for future changes and releases that have the potential to impact existing baseline configuration

Position 9. E-Discovery Administrator (Security/FOIA/CAPSTONE):

DESCRIPTION:

This position has been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 612 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. The contractor shall perform tasks associated with legal discovery and data archival in the IL4/IL5/Il6 environments. Additionally, the contractor will respond to reported electronic spillage of classified data and take approved remedial action.

QUALIFICATIONS REQUIRED:

- Clearance requirement is TOP SECRET
- 3+ years IT experience with significant experience with Microsoft 365 Admin Center
- Azure Fundamentals Certification
- Microsoft 365 Fundamentals Certification
- Microsoft Security, Compliance, and Identity Fundamentals Certification
- Relevant experience as a Microsoft Exchange administrator
- Relevant experience as a Microsoft Teams administrator
- Relevant experience as a Microsoft SharePoint administrator
- Relevant experience as a Microsoft OneDrive administrator
- Knowledge and experience with Microsoft Intune
- Experience with ACAS server maintenance and configuration
- Understanding of cloud computing and networking
- Experience supporting Splunk
- Superior organizational skills
- Capable of managing multiple projects
- Great communication skills (oral and written)
- Strong attention to detail

- Working knowledge of the Information Technology Infrastructure Library (ITIL) Framework
- Completion of Federal Law Enforcement Training Center Digital Forensics Levels 1 & 2 or equivalent Digital Forensic Examiner certification (*for contractor employees performing data discovery and archival and prepare for transfer to legal authorities*)

CONTRACTOR SHALL:

- Take administrative action in response to reported electronic spillages of classified data, to include content search, quarantine, creating archival copies, and/or deletion of data
- Manage user data retention policies, to include placing data in litigation hold
- Perform data discovery and archival and prepare for transfer to legal authorities
- Enable/disable user accounts yeard on information assurance events in coordination with Information Systems Security Managers
- Analyst shall provide knowledgeable and skilled in FOIA, Privacy, and records management processing (analyzing requests and exemptions, writing correspondence, managing workload)
- Analyst will utilize FOIA, Privacy, and records management governing documents, to complete tasks
- Analyst shall process requests and reviews for all public release programs to include but not limited to FOIA/PA and records management
- Execute Privileged User (PU) management process (e.g., receive and analyze PU requests, ensure requests are thorough and justified, ensure requirement is validated per DON/USN directives).
- Conduct audits of various security elements of the IL6 tenant covering topics such as vulnerability remediation, endpoint security posture, Conditional Access Policies, role assignments and trust relationships.
- Manage and operate cloud-based Comply-to-Connect/Enhanced Network Access Control (eNAC) system (e.g., design and implement policies, attend DoD level forums to capture requirements)
- Support personnel investigations and litigation-related account requests and data delivery
- Brief various audiences on IL6 management efforts and maneuvers as needed
- Manage infrastructure devices (e.g., routers, switches, Firewalls) that support Splunk
- Provide the following services when required by the Government and as directed in writing by DON credentialed, badged, or appointed investigators within 72 hours from the time of the investigator's request unless another timeline is indicated. Confirm within 48 hours receipt of direction in writing to the PCO:
    - Electronic Information File (EIF) retention, recovery, and archiving
    - Internet and Intranet Activity Monitoring
    - Single POC for Law Enforcement/Criminal Investigations (LE/CI) support services
    - Securing End User EIF
    - Documentation of Services Provided
    - Delivery Formats and Delivery Locations
    - Confidentiality

    - Privacy
    - Under exigent circumstances and in response to threats to national security, allow duly authorized Government personnel to seize data, SW, HW, and associated peripheral devices found to be of evidentiary value to an investigation.
    - LE/CI Support
    - Compliance with DON policies specifying the roles and responsibilities of the Naval Criminal Investigative Service
- Provide technical advice and assistance for the following:
    - Assist DON attorneys in responding to subpoenas, discovery requests, court orders, and other matters related to litigation
    - Respond within 10 calendar days (or 20 calendar days in the case of retrieving information from network backup tapes) from the date of the DON lead attorney's written request
    - Provide Litigation Support services
    - Provide Litigation Holds services
    - Provide Record Search and Production Services
    - Provide Testimony Services
    - Provide Advice and Assistance to Government Attorneys in preparing for and presenting the Government's case at trial
    - Adhere to provisions related to the Confidentiality and Release of Government Information
    - Comply with relevant Privacy Act and FAR provisions

Position 10. Identity and Entitlement Administrator:

DESCRIPTION:

This position has been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 612 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. The contractor shall perform tasks associated with account management for users and administrators, to include user account provisioning and de-provisioning, administrator account creation and deletion, and assignment and management of Role-Based Access Control permissions for administrator accounts.

QUALIFICATIONS REQUIRED:

- Clearance requirement is TOP SECRET
- 3+ years IT experience with significant experience with Microsoft Azure
- Azure Fundamentals Certification
- Microsoft 365 Fundamentals Certification
- Azure Administrator Certification
- Understanding of cloud computing and networking
- Experience with Microsoft Office suite and PowerShell
- Superior organizational skills
- Capable of managing multiple projects

- Great communication skills (oral and written)
- Strong attention to detail
- Working knowledge of the Information Technology Infrastructure Library (ITIL) Framework

CONTRACTOR SHALL:

- Provision, de-provision, and manage user identities using the DISA Defense Enterprise Provisioning Online (DEPO) tool or analogous future tool
- Monitor Azure Active Directory audit logs to ensure identities are properly synchronizing from DISA Global Directory Services to Flank Speed via Azure Active Directory Connect
- Perform user migration data pre-screening
- Create, modify, and remove administrator accounts and applicable roles as directed
- Troubleshoot and correct user identity issues as required, to include interface with mission partners and DISA

Position 11. Personnel Security Specialist:

DESCRIPTION:

This position has been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 75 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. The contractor shall perform tasks associated with conducting employee background checks and security clearance investigations.

QUALIFICATIONS REQUIRED:

- Clearance requirement is SECRET\GENSER
- 3+ years of experience
- Strong attention to detail
- Strong organizational skills, with the ability to work on multiple projects with multiple deadlines
- Must be a fast learner and self-starter
- Excellent written, verbal, visual/presentation, interpersonal and communications skills
- Ability to consistently make good decisions through a combination of analysis, wisdom, experience, and judgment
- MS Office and the ability to navigate between multiple programs simultaneously

CONTRACTOR SHALL:

- eQIP package reviews for accuracy and completeness
- eQIP package submittals, tracking, updating, validations, and corrections
- Manage receipt of security documents submitted from applicants

- Verify the appropriate level of background investigation being requested
- Ensure all documents required for suitability processing are included and completed properly
- Conduct agency checks and evaluate results including but not limited to credit reports and processing fingerprint cards
- Identify potential reciprocity and previous investigations
- Identify issues on security forms and obtain any missing information from applicant
- Provide customer service to internal and external customers via email and of phone
- Assist other teams (Investigations, EOD, File Room, etc.) on special projects as needed

Position 12 Financial Specialist

DESCRIPTION:

This position has been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 75 and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. The contractor shall perform tasks associated with conducting employee background checks and security clearance investigations.

QUALIFICATIONS REQUIRED:

- Clearance requirement is SECRET\GENSER
- 3+ years of experience
- Strong attention to detail
- Strong organizational skills, with the ability to work on multiple projects with multiple deadlines
- Must be a fast learner and self-starter
- Excellent written, verbal, visual/presentation, interpersonal and communications skills
- Ability to consistently make good decisions through a combination of analysis, wisdom, experience, and judgment
- MS Office and the ability to navigate between multiple programs simultaneously

CONTRACTOR SHALL:

- Provide direct support in the formulation, justification, and execution of the command's annual budget and spend plan.
- Monitor and track the commitment, obligation, and expenditure of funds in accordance with the command’s financial milestones and report discrepancies to government personnel.
- Utilize government-provided financial management systems (e.g., GFEBS, DTS) to process, record, and reconcile financial transactions, including purchase requests and travel orders.
- Generate and consolidate weekly and monthly financial status reports, budget execution summaries, and variance analyses for review by command leadership.

- Assist in the preparation of Unfunded Requirements (UFRs) and reprogramming requests by gathering and validating supporting data.
- Support the end-of-year closeout process by ensuring all financial actions are completed, documented, and reconciled in a timely manner.
- Provide assistance to command staff in resolving routine financial inquiries and ensuring adherence to Joint Travel Regulations (JTR) and other financial policies.

Position 13 Information Assurance Analyst

DESCRIPTION:

These positions have been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 641, and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2. The Information Assurance (IA) Analyst is responsible for ensuring the confidentiality, integrity, and availability of information systems by managing the security and compliance framework across the enterprise cloud and network infrastructure. This role serves as the subject matter expert on risk management and compliance, translating federal and DoD security directives into actionable controls and procedures. The IA Analyst continuously monitors the security posture, manages vulnerabilities, and maintains the formal documentation required to achieve and sustain the Authority to Operate (ATO). This individual acts as the critical link between operational/engineering teams and the formal security accreditation process for both on-premise network services and cloud environments.

QUALIFICATIONS:

Must have a minimum of five (5) years of dedicated experience in Information Assurance or Cybersecurity. This experience must include:

- Clearance requirement is TOP SECRET
- Direct, hands-on application of the Risk Management Framework (RMF) from initiation to continuous monitoring.
- Experience conducting vulnerability assessments using tools such as ACAS, Nessus, or equivalent systems.
- Experience implementing and auditing systems against Security Technical Implementation Guides (STIGs).
- At least two (2) years of experience must involve securing cloud environments (e.g., AWS, Azure) and a working knowledge of FedRAMP controls.
- must hold a certification meeting DoD 8570/8140 IAM Level II requirements (e.g., CompTIA CASP+, CISM, or CISSP).

CONTRACTOR SHALL:

- Shall manage and maintain the security posture of enterprise cloud and network services throughout all phases of the Risk Management Framework (RMF) lifecycle.

- Shall conduct regular vulnerability scans of network and cloud assets using government-approved tools, analyze scan results, and coordinate with technical teams to prioritize remediation actions.
- Shall perform continuous monitoring and compliance validation of network devices, servers, and cloud resources against Security Technical Implementation Guides (STIGs) and other agency-specific benchmarks.
- Shall analyze and verify compliance within the enterprise cloud environment (e.g., AWS, Azure), ensuring alignment with FedRAMP controls and proper implementation of the shared responsibility model.
- Shall develop, update, and maintain all necessary RMF documentation, including the System Security Plan (SSP), security control traceability matrices, and Plans of Action and Milestones (POA&M).
- Shall serve as a primary point of contact for internal and external security audits, responsible for gathering and presenting evidence of control implementation to auditors.
- Shall track, interpret, and report on Information Assurance Vulnerability Management (IAVM) directives, coordinating with technical teams to ensure timely remediation and reporting.
- Shall provide information assurance expertise and guidance to network and cloud engineering teams to ensure security controls are integrated into the design and implementation of new services ("security by design").

Position 14 Network Specialist

DESCRIPTION:

These positions have been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 641, and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2 The Tier 2 Network Specialist is responsible for the advanced operational support, management, and troubleshooting of the enterprise network infrastructure, with a specific focus on transport services (e.g., MPLS, VPLS, Carrier Ethernet) and the Software-Defined Wide Area Network (SD-WAN) environment. This role serves as a critical escalation point for the Tier 1 help desk, handling complex incidents, performing planned network changes, and ensuring the reliability, availability, and performance of the enterprise network. The specialist will work closely with Tier 3 engineering teams to resolve persistent issues and contribute to the overall stability and optimization of the network.

QUALIFICATONS:

- Clearance requirement is TOP SECRET
- 3+ years of hands-on experience in a network operations or network engineering role within an enterprise environment
- Demonstrated experience managing and troubleshooting WAN and LAN technologies, including routing protocols, and switching
- At least 2 years of direct experience with SD-WAN solutions. This includes provisioning,

policy creation, and troubleshooting
- Proven experience working with telecommunications providers to troubleshoot and resolve issues with commercial and carrier transport services like MPLS, Metro Ethernet, or broadband
- Experience using network monitoring and management tools to diagnose and resolve network issues.
- Cisco Certified Network Associate (CCNA) or Cisco Certified Network Professional (CCNP)
- SD-WAN specific certifications (e.g., Cisco SD-WAN Solutions, VMware VeloCloud)
- CompTIA Network+

CONTRACTOR SHALL:

- Provide Tier 2 operational support for the enterprise network, serving as the primary escalation point for unresolved incidents from Tier 1 related to transport and SD-WAN services
- Perform advanced troubleshooting and fault isolation to resolve network outages and performance degradation issues, and document all actions taken in the government-provided ticketing system
- Manage, configure, and maintain the SD-WAN environment, including implementing application-aware routing policies, traffic shaping rules, and security policies as directed by government personnel
- Act as the technical liaison with telecommunications carriers and service providers to report and resolve transport circuit issues, including coordinating dispatched technicians and testing
- Utilize network monitoring tools to proactively identify, analyze, and report on network performance, availability, and utilization trends for all WAN and SD-WAN links
- Implement, and verify approved network configuration changes, including router/switch configurations, firewall rule modifications, and SD-WAN policy adjustments, in accordance with established change management procedures
- Maintain accurate and up-to-date documentation of the network infrastructure, including network diagrams, device configurations, and circuit information
- Support the Tier 3 engineering team by gathering diagnostic data, performing tests, and assisting in the resolution of complex or persistent network problems

Position 15 Network Analyst

DESCRIPTION:

These positions have been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 641, and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2 Mid-Level Network Analysts is responsible for ensuring the stability, integrity, and efficient operation of the enterprise network. This hybrid role provides advanced Tier 2 operational support for

complex incidents and service requests while also participating in Tier 3 activities. The analyst will lead troubleshooting efforts for difficult or recurring issues, perform root cause analysis, and work closely with senior network engineers on network optimization, design, and automation initiatives. This position is the primary escalation point for junior specialists and is expected to resolve all but the most complex network problems that would require architectural changes.

QUALIFICATIONS:

- Clearance requirement is TOP SECRET
- 5+ years
- In-depth, hands-on experience with the design, implementation, and operation of complex WAN/LAN environments, including advanced routing (BGP, OSPF) and switching.
- At least 3 years of direct, in-depth experience with SD-WAN architecture, deployment, and management, including advanced policy creation and overlay/underlay troubleshooting.
- Extensive experience leading troubleshooting efforts with telecommunications providers for chronic or complex transport circuit issues (MPLS, Carrier Ethernet, 5G/LTE).
- Demonstrated ability to perform root cause analysis (RCA) and develop long-term solutions to recurring network problems.
- Experience with network automation concepts and scripting is strongly desired.
- Cisco Certified Network Professional (CCNP) or equivalent advanced certification is strongly preferred.
- Advanced SD-WAN certifications (e.g., Cisco Certified Specialist - Enterprise SD-WAN Implementation).
- CompTIA Network+ / Security+

CONTRACTOR SHALL:

- Serve as the senior technical lead for Tier 2 operations, handling the most complex incidents and providing guidance to junior analysts for issues related to transport and SD-WAN services
- Lead and conduct comprehensive root cause analysis (RCA) for major network incidents and recurring problems, delivering detailed findings and actionable recommendations to government leadership
- Collaborate with the Tier 3 engineering team on network design, optimization, and capacity planning efforts by providing operational insights and performance data
- Develop, test, and deploy advanced SD-WAN policies for application traffic steering, quality of service (QoS), and security in collaboration with network architects
- Author and maintain standard operating procedures (SOPs), technical diagrams, and knowledge base articles for complex network configurations and troubleshooting techniques
- Assist in the evaluation, testing, and integration of new network technologies, software versions, and hardware platforms before enterprise-wide deployment
- Develop and maintain scripts and automation tools to streamline routine network monitoring, reporting, and configuration tasks

- Function as the primary technical escalation point for all network operational matters before engaging vendor support or Tier 3 architects

Position 16 Network Engineer

DESCRIPTIONS:

These positions have been designated as a Cyber IT/Cybersecurity Workforce position in Specialty Area 641, and as a condition of employment incumbents of the position is required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2 The Senior Network Engineer functions may have multiple focus on transport, SD-WAN, and firewall management. This role is responsible for overseeing the service delivery, operational readiness, and incident command for these specific domains in support of the ordering activity. This individual ensures the stability, availability, and performance of the live network by leading the operational teams, enforcing established standards, and managing the service lifecycle of these core functions, ensuring real-time network operations, orchestrating the response to all service disruptions impacting transport, SD-WAN, or security infrastructure.

QUALIFICATIONS:

- Clearance requirement is TOP SECRET
- 5-7+ years of experience
- ITIL v4 Foundation certification and a certification meeting DoD 8570/8140 IAT Level II requirements (e.g., CompTIA Security+)
- Certifications such as ITIL v4 Managing Professional, CISSP, CCNP Enterprise/Security, or PCNSE are highly desired to demonstrate a strong understanding of both the operational framework and the underlying technologies

CONTRACTOR SHALL:

- Serves as the operational authority for all network transport, SD-WAN, and firewall services, overseeing day-to-day service delivery and ensuring adherence to architectural standards
- Acts as the primary Incident Commander during Major Incidents affecting network services, directing the activities of all technical response teams and orchestrating the overall service restoration effort
- Provides authoritative operational status, mission impact assessments, and situational reports to government leadership during network service disruptions
- Owns, maintains, and refines the operational playbooks, Standard Operating Procedures (SOPs), and incident response procedures for the transport, SD-WAN, and firewall operations teams
- Oversees the Problem Management process for network services, ensuring that government-approved root cause analyses for complex or recurring network issues are completed and that remediation plans are tracked to successful completion

- Represents operational interests as a primary stakeholder in the Change Advisory Board (CAB) process, responsible for assessing the operational risk of all proposed changes to the network and security infrastructure
- Manages, monitors, and reports on network Service Level Agreement (SLA) performance related to transport availability, SD-WAN performance, and firewall uptime
- Provides mentorship and guidance to junior staff focused on operational best practices and disciplined incident management related to the network infrastructure

11.0 QUALIFICATION REQUIREMENTS:

Relevant to all positions on this PWS, under "Qualifications required", years of experience are clearly delineated. In this delineation, the following is a hard requirement. Where it states:

- 7+ years' experience – contractor filling position SHALL possess and reflect solid and cumulative employment for 6 of those 7+ years. Aforementioned 6 year, solid and cumulative employment start date will be dated no further than 7 years back from date of contract award.
- 5+ years' experience - contractor filling position SHALL possess and reflect solid and cumulative employment for 5 of those 5+ years. Aforementioned 5 year, solid and cumulative employment start date will be dated no further than 6 years back from date of contract award.
- 3+ years' experience – contractor filling position SHALL possess and reflect solid and cumulative employment for 3 of those 3+ years. Aforementioned 3 year, solid and cumulative employment start date will be dated no further than 4 years back from date of contract award.
- 1+ years' experience – contractor filling position SHALL possess and reflect solid and cumulative employment for 1 of those 1+ years. Aforementioned 1 year, solid and cumulative employment start date will be dated no further than 2 years back from date of contract award.

12.0 TRAVEL REQUIREMENTS

There is a minimal amount of travel required in support of this task order, only a select few positions shall be required to travel. All travel costs incurred shall be separately priced and executed in accordance with the Federal Travel Regulations (FTR). This directive can be accessed at http://www.gsa.gov/portal/ext/public/site/FTR/file/FTRTOC.html/category/21865/hostUri/portal.

A copy of all travel requests shall be routed to the COR prior to execution. Upon validation of the travel requirement, the COR will forward the travel request to the CONTRACTOR with Government approval. Any travel not directly related to this requirement, or not validated by the COR, is not chargeable to the Government. Upon return from travel, the CONTRACTOR shall prepare a Travel/Trip Report providing the accomplishments of the travel.

13.0 TRANSITION PLAN

A Transition/Phase-in plan is required to ensure continuity of services to the successor in FY 2027. The plan shall include phase-in activities to be accomplished during the final one month of the current contract end date (25 February 2027). After the contract is awarded, the successor shall conduct knowledge transfer with the incumbent for a period of thirty (30) days, within the phase-in period. This phase is designed to ensure a flawless transition of services. Immediately upon winning the task order the contractor will review all tasks specified within it. Before the contract kick-off meeting, the successor, in consultation with the Government, will create an action plan. This plan is crucial for ensuring the smooth transition of services. By the end of this phase-in period, the contractor will be fully responsible for executing the contract terms.

13.1 Phase-In / Mobilization Phase

During this mobilization period, the contractor shall:

- Present a sound program and project management approach that will successfully transition requirements within the stated transition period with no degradation to services.
- Ensure all watch floor operator positions on the PWS are filled, adequately trained and qualified to maintain all 24/7/365 IL5/IL6 Cloud Support and Services by the end of the mobilization period.
- Ensure system security and successfully accomplish the requirements of the PWS and delivery of contract deliverables.
- Identify through submission of a Manning Chart, which will include key position personnel, to include Shift Leads, Technical Leads, and Training Leads, and ensure all identified personnel are qualified and possess the necessary knowledge and skills to perform in identified position.
- Submit a watch bill that identifies watch floor operators name, position filled and shift which will culminate in 24/7/365 Cloud Support and Services.
- Ensure personnel have read and understand all applicable directives relating to the NAVNETWARCOM IL5/IL6 Flank Speed and Cloud Operations mission. Directives include but are not limited to OPORDS, EXORDS, TASKORDS, CONOPS, and specific mission tasking's.
- Ensure technical lead personnel are able to continue producing all operational documents.
- Ensure technical lead personnel are able to create and distribute all current reports.
- Ensure all personnel have necessary access to systems/sites required to perform mission.
- Ensure personnel are familiar with all NAVNETWARCOM and IL5/IL6 standard operating procedures (SOP) currently in use.
- Ensure personnel are familiar with Navy rank structure and organization, to include TYCOM, SYSCOM, PORs, Shipboard organization, Fleet commanders, Squadron commanders, etc.
- Ensure that the appropriate background investigations as required of this PWS have been completed, and if not, ensure that the necessary documentation is completed and submitted prior to the end of the mobilization period.
- Inability to hold a Secret clearance and/or be issued a CAC is considered disqualifying

for any candidate. The contractor shall ensure that all prospective operators obtain all appropriate identification cards during the mobilization period.
- In the event that the contractor plans on hiring incumbent SMEs, the contractor is responsible for ensuring that the background investigations for those personnel are compliant, and any discrepancies identified are resolved prior to the end of the mobilization period.

Should the incumbent contractor not be selected as the follow-on service provider, as applicable, the contractors shall participate in a transition phase to orderly and efficiently transition to a successor. The transition phase shall be considered the last thirty (30) days prior to the end of the contract period of performance. The transition phase shall consist of the following:

- Provide phase-in training for the successor.
- Provide access to all training, operations, and technical documentation relevant to the mission.
- Provide key personnel specific turnover for lead positions. At a minimum, ensure a sufficient turnover of technical lead personnel, training personnel, and shift lead personnel with incoming counterpart.
- Provide point of contacts for all necessary task functions.

14.0 MISSION ESSENTIAL:

Some positions maintain a requirement for Mission Essential.

Mission Essential services are those that shall be performed in the event of emergencies, inclement weather, and natural or manmade disasters (e.g., hurricanes, snowstorms, tornadoes, fire, or emergency rescue efforts). This also includes all State and Federal Holidays. Consequently, certain positions filled by CONTRACTOR personnel in accordance with this PWS may be determined to be Mission Essential. CONTRACTOR employees who are determined to be Mission Essential SHALL provide services during time of emergency, inclement weather, and natural or manmade disaster. Even if the road conditions are hazardous, Mission Essential CONTRACTOR employees are expected to report on time unless otherwise officially authorized by the COR.

CONTRACTOR employees who are on-shift at the time an event of emergencies, inclement weather, and natural or manmade disasters (e.g., hurricanes, snowstorms, tornadoes, fire, or emergency rescue efforts), occurs, may be required to stay on-shift until replacement CONTRACTOR employees are able to safely respond to the compound.

The Government shall specify Mission Essential positions. The CONTRACTOR shall provide a minimum of 25% manning of watch floor positions. Each area of expertise is expected to have coverage at all times. At NO TIME, shall there be less than two (2) CONTRACTOR employees on the watch floor at any time.

If Mission Essential CONTRACTOR employees are unable to perform as required in the event of an emergency, inclement weather, and natural or manmade disasters, they SHALL immediately report that to their Contracting Company Program Manager. The Contracting Company Program Manager shall then contact the COR to report the situation, and to ask for further guidance. Such guidance can include either approval to not report as required or approval for late arrival.

See table below with mission essential personnel labor categories.

Position Number	Labor Category	
Position 4	Azure Virtual Desktop Sys Admin	
Position 5	Cloud Service Support Admin/Analyst	
Position 6	Cloud Service Support Engineer	
Position 7	Cloud Application Admin	
Position 14	Network Specialist	
Position 15	Network Analyst	

15.0 DELIVERABLES

The Contractor shall provide the deliverables listed below in accordance with this Performance Work Statement (PWS). All deliverables shall be complete, accurate, and submitted in the specified format by the required due date. Unless otherwise directed by the Government, all documentation shall be unclassified, written in clear and concise English, and delivered in Microsoft Office 365-compatible formats (.docx, .xlsx, .pptx, .pdf) or approved equivalents.

15.1 Contractor Quality Assurance Plan (QASP)

Due within 30 days of period of performance start and updated annually. Plan shall describe methods to monitor and ensure contract compliance.

15.2 Monthly Status Report

Due to the COR and Technical Lead no later than the 20th day of each month. Report shall include:
a. Task/project status (originator, personnel assigned, goal/end-state, estimated completion date, percent complete)
b. Personnel issues
c. Anticipated activity for next period

15.3 Contract Kick-Off Meeting

The Contractor shall conduct a kick-off meeting within 5 days of contract award. Minutes and action items must be approved by the Government and distributed.

15.4 Program Management Plan (PMP)

Draft PMP presented at Kick-Off Meeting; final PMP due within 30 calendar days after Government feedback. PMP shall be kept current and briefed upon request.

15.5 Trip Reports

Trip reports shall include purpose, participants, outcomes, and recommendations.

15.6 Specific Work Products

Contractor shall provide operational and technical work products including, but not limited to:

- Updates to TTPs/SOPs
- Deployment of system patches
- Validation of IA controls
- Monthly operational dashboards and metrics
- Incident and problem management reports
- Configuration baseline reports
- Service performance and trend reports
- Audit logs and compliance reporting for cloud, M365, Intune, SD-WAN
- Tenant, endpoint, and network operational summaries
- Security and vulnerability assessment reports
- Operational knowledge management repository updates

15.7 Monthly Financial Report

Submitted no later than 10 business days after month-end. Shall include invoices submitted but unpaid, cost tracking, and analysis.

16.0 TRAINING REQUIREMENTS AND OPPORTUNITY:

The Government Technical Lead and COR are responsible to permit contracting resources to attend (NO COST) training and other opportunities to enhance the employee's ability to perform their assigned tasks at a higher level of proficiency and accuracy. This includes but is not limited to attending COMMAND\DEPARTMENTAL\DIVISIONAL offsite events when hosted by the Government as “assigned place of duty”.

AT COST training will have funding provided for training by the Contracting company and will be coordinated through the Technical Lead and COR to ensure appropriate coverage is provided to complete the expected level of work without exception.

17.0 ASSOCIATE CONTRACTOR AGREEMENTS (ACA) FOR ENTERPRISE OPERATIONS

(a) The Government selected a multi-award, collaborative integrator approach for the Enterprise Operations IDIQ contract. The successful performance of this contract requires that the awardees

work in close cooperation as a unified team. Therefore, each awardee of this IDIQ contract shall be required to enter into an Associate Contractor Agreement (ACA) with all other awardees.

(b) The purpose of the ACA is to establish the framework for collaboration, communication, and integration among the awardees to ensure the seamless delivery of services to the Government. The ACA shall, at a minimum, address the following areas:

(1) Roles and responsibilities of the Associate Contractors.
(2) A governance structure, such as a Government Led Council set in place, for managing technical dependencies and resolving issues.
(3) Requirements and procedures for the exchange of technical data, proprietary information, and performance metrics necessary for the integrated performance of all contract-related duties.
(4) A multi-tiered dispute resolution process that prioritizes technical-level resolution and provides a final adjudication path through the Government Program Manager.
(5) Procedures for the protection of proprietary data.

(c) The Government reserves the right to review the ACA and may require modification if it is found to not be in compliance with the intent of this clause or if it is determined to be prejudicial to the Government's interests.

(d) Refusal to enter into an ACA by any awardee may be grounds for termination of their IDIQ contract for cause in accordance with FAR 52.212-4(m). Compliance with the terms of the executed ACA is a material requirement of the contract. Failure to comply with the terms of the ACA may negatively impact past performance evaluations (CPARS) and may be considered when awarding future task orders.

18.0 ORGANIZATIONAL CONFLICT OF INTEREST (OCI) - IDIQ

1.0 Purpose and Incorporation of FAR Guidance
This clause is intended to ensure that the Contractor's performance under this IDIQ Agreement is conducted with complete impartiality and without any actual or perceived conflict of interest, in accordance with the principles set forth in Federal Acquisition Regulation (FAR) Subpart 9.5.

2. Definition
An *Organizational Conflict of Interest (OCI)* exists when, due to other activities, relationships, or contracts, the Contractor is unable or potentially unable to render impartial assistance or advice to the Government, the Contractor's objectivity in performing the contract work is or might be otherwise impaired, or the Contractor has an unfair competitive advantage.

3. Contractor Obligations & Non-Disclosure

- Disclosure: The Contractor shall promptly disclose in writing to the Contracting Officer any actual or potential OCI upon discovery at any time during the life of this IDIQ.
- Mitigation: The Contractor shall take all reasonable steps, including submitting a formal

OCI Mitigation Plan as directed by the Contracting Officer, to avoid, neutralize, or mitigate the conflict.

- Protection of Information: If the Contractor requires access to proprietary data of other companies or non-public Government information to perform this contract, the Contractor shall enter into agreements to protect such data and refrain from using the information for any purpose other than that for which it was intended (per FAR 9.505-4).

- 4. IDIQ Task Order Applicability

Because this is an IDIQ contract, OCI will be continually evaluated at the Task Order level.

- Prior to the award of any Task Order, the Contractor may be required to certify that no OCI exists related to the specific statement of work.
- If a Task Order requires the Contractor to draft specifications, requirements, or evaluate systems developed by themselves or competitors (as illustrated in FAR 9.508), the Contractor may be excluded from subsequent Task Orders or follow-on acquisitions to prevent biased ground rules or impaired objectivity.

- 5. Government Remedies

If the Contractor fails to disclose an OCI, misrepresents relevant facts, or fails to resolve an OCI to the satisfaction of the Contracting Officer, the Government may take appropriate action, including but not limited to:

- Disqualification from bidding on specific Task Orders.
- Termination of the applicable Task Order or this base IDIQ Agreement for default.
- Disqualification from future related Government solicitations.

- 6. Survival

The obligations regarding the protection of non-public or proprietary information, and the restrictions on future contracting based on work performed under this IDIQ, shall survive the completion or termination of this Agreement.