Performance Work Statement
United States Marine Corps Education Command Information Technology Support Services (EDCOM ITSS)

1. BACKGROUND. Marine Corps Education Command (EDCOM) Information Technology (IT) Directorate is tasked with providing the full scope of information technology services in support of the command's operations and professional military education. EDCOM's IT systems and services are provided via a hybrid environment consisting of an on-premises data center located within the Warner Center and a Microsoft Impact Level 2 (IL2) Azure cloud environment. Office automation services are provided via Microsoft M365. EDCOM IT maintains a wired .edu network as well as a wireless Bring Your Own Device (BYOD) network known as CampusNet both at Quantico the five Staff NCO Academies and the seven College of Distance Education and Training (CDET) Regional Campus locations across the US and in Japan. These facilities require a significant level of support. EDCOM is also leading the USMC's effort to include Joint All Domain Operations (up to the Secret and SCI levels), Wargaming, and the adoption of Artificial Intelligence (AI) into professional military education.

2. SCOPE. EDCOM has a requirement for information technology support services across the Command, as managed by the Information Technology (IT) Directorate in its mission to provide information technology support services.

3. OBJECTIVES. The primary objectives for this requirement are as follows:

3.1. Network and System Support: Provide support for the installation, configuration, maintenance, sustainment, operation, troubleshooting, monitoring, reporting, security compliance assessing and administration of all IT systems, services, applications, hardware, infrastructure, circuits, data centers and networks under the control of EDCOM.

3.2. Technical Support: Provide IT technical customer support as the primary interface for user support, providing helpdesk operations support, initial triage, in-person and remote troubleshooting, account creation, administration and troubleshooting, end user device and application troubleshooting, trouble ticket creation and management, issue escalation, and end user device imaging.

3.3. Cybersecurity and Information Security: Provide Cyber-Security support and oversight of all EDCOM systems ensuring network security and compliance.

3.4. Audiovisual & Video Teleconference (AV/VTC) Support: Provide user level configuration, preventative maintenance, functionality and operation checks, operation, status reporting, monitoring, inventorying, and user level troubleshooting of Audio Visual and Video Teleconference (AV/VTC) equipment and systems.

4. GENERAL REQUIREMENTS.

4.1. The Contractor shall provide comprehensive capabilities to support mission accomplishment. Collectively, the Contractor shall provide support services across all task areas included in this requirement (see section 5 below).

4.2. Performance Management. The Contractor shall provide the necessary resources and infrastructure to manage and administer the performance under this effort. The selection of teaming partners, subcontractors, facilities, and other business considerations is discretionary on the part of the Contractor. The Contractor shall establish processes and assign appropriate management and support resources to

DRAFT

administer the resulting contract, to include management of subsequent task orders, staffing actions, subcontractor management, and financial matters. The Contractor shall interface with the Government's Contracting Officer Representative (COR), the Director of IT, and other designated EDCOM staff. At all times, the prime Contractor shall be responsible for the actions of their teaming partners and subcontractors. The Government will not consider the roles of the task order support staff as direct charge elements of performance.

4.3. Technical Performance Quality. The Contractor is responsible for providing the management and staff capable of handling the responsibilities of task order execution and coordination of team resources. Task leads may be appointed from among team member; however, the technical cognizance over performance remains with the prime Contractor. At all times the prime Contractor is responsible for all personnel resources, performance quality, and deliverables associated with a task order.

4.4. Management Performance. The Contractor shall support all facets of technical performance with a sound management structure that ensures cost-effective support to EDCOM in the execution of its mission. Throughout the task order performance, the Contractor is responsible for ensuring that assigned staff members are executing responsibilities in consonance with the PWS requirements and associated quality standards. The Contractor will coordinate all correspondence with the EDCOM Contracting Officer Representative (COR).

4.5. Staffing Requirements. The Contractor shall be responsible for staffing, competency training, guidance, and supervision of qualified personnel performing under the resulting task order. The Contractor shall accomplish the assigned work by employing and utilizing qualified personnel possessing an appropriate combination of education, training, and experience required to respond to the PWS criteria. No waivers will be proposed or considered. Staff initially assigned shall provide the benchmark for replacement staff qualifications and no dilution of such qualifications, or reduction in performance shall be incurred by the Government because of staff reassignment/departure.

4.6. Personnel. The Contractor shall be responsible for employment, training, guidance, and supervision of qualified personnel performing under this task order. The Contractor shall accomplish the assigned work by employing and utilizing qualified personnel possessing an appropriate combination of education, training, and experience to successfully accomplish this contract. No waivers will be proposed or considered. The Contractor shall be responsible for ensuring all employees and sub-contractors (if used) adhere to all Government guidance and orders related to public health and pandemic response and reporting, including but not limited to social distancing, wearing of masks, quarantining, and vaccinations.

4.7. Government Interface. The Contractor shall establish and maintain the necessary interfaces with Government staff required to execute their program strategy. The Contracting Officer will assign a designated COR who will have cognizance over all tasks and execute responsibilities for technical oversight of performance, deliverables acceptance, invoiced certification, and coordination of follow-on work efforts. The Regional Contracting Office Procurement Contracting Officer (RCO PCO) will interface with the Prime Contractor representatives for payment and administration.

4.8. Place of Performance. The Contractor shall provide services at Government sites. The place of performance for this effort is EDCOM facilities located in:

MCB Quantico, Virginia
MCB Camp Lejeune N.C., (Camp Johnson N.C.)
MCB Camp Pendleton, CA
Marine Corps Air Ground Combat Center, Twentynine Palms, CA

DRAFT

MCB Hawaii, HI
MCB Okinawa, JP
MCAS Miramar/MCRD San Diego, CA **
Joint Reserve Base Fort Worth, TX **

** Support at this site will be provided remotely or via contractor travel to the site.

The Contractor will be required to follow the established base access control policies and procedures for each location.

The place of performance for this effort is physically at the Government site. For situations in which base or facility closure occurs due to emergencies, health events (e.g. COVID-19), weather related events, and other unusual circumstances which prevent performance at the government site the Contractor may provide services remotely at the discretion and written approval by the Contracting Officer Representative.

4.9. Government Site Office Space: The Government will provide the following desks allocation for the contractor to execute the services on task orders:

Location	Number of Desks Available
Quantico, VA	23 Desks
Camp Lejeune N.C (Incl Camp Johnson, N.C.)	1 Desk
Camp Pendleton, CA	1Desk
Hawaii	1 Desk
MCAGCC Twenty-nine Palms, CA	1 Desks
Okinawa, Japan	1 Desk
MCAS Miramar, CA	0 Desks **
Joint Reserve Forth Worth (FTW), TX	0 Desks **

** Support at this site will be provided remotely or via contractor travel to the site.

4.10. Hours of Operations. Most of the services shall be performed during normal working hours of 0730-1700 Local, Monday through Friday however, weekend and after-hours support may be required due to mission requirements. Weekend and after-hours support will not exceed 5% of the support required. Users may request support in person, by telephone, by e-mail or trouble ticket entry into a help desk system. Visits by the Contractor to user office spaces within EDCOM facilities.

4.11. Travel. Government-directed travel will be reimbursed in accordance with (IAW) Revolutionary Federal Acquisitions Regulation Overhaul (RFO) 31.205-46 (a) (2). Any travel costs exceeding those allowed under Joint Travel Regulation will not be reimbursed. All reimbursable travel will be approved by the COR. Itemized receipts from travel must be maintained by the Contractor and submitted to the COR or contracting officer with each associated invoice upon request. The chart below outlines the expected yearly travel. Yearly travel shall not exceed the Travel ODC CLIN amount stated in the award.

4.12. Common Access Card (CAC) Issuance: Both physical and logical access (network logon) is the requirement to qualify for CAC issuance for Contractors who need access to, or are stationed on, bases/facilities that use Navy Access Control System (NCACS). If both physical and logical access is deemed warranted, then the Government will sponsor the Contractor for the issuance of a CAC. Within 10 calendar days of the task order award, the Contractor must identify those personnel to the COR for

DRAFT

whom the Contractor can justify requiring physical and logical access. Personnel without a favorably adjudicated clearance are ineligible for a CAC.

4.13. Quarterly Performance Review Conferences: On a quarterly basis, the Contractor shall coordinate and facilitate performance review conferences. At these conferences, the Contractor shall discuss with the Contracting Officer and COR any performance matters, lessons learned, or concerns identified with contractor performance. Additionally, the Contractor shall report any cyber security incidents faced by the contractor in their network IAW with DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. The Contractor will provide meeting minutes to the COR within 7 days following each Quarterly Performance Review Conference.

4.14. Security Requirements.

4.14.1 Most of the work carried out at EDCOM facilities is performed in unclassified work areas. However, some of the work will be in controlled access information technology spaces (e.g., data centers) with access to sensitive information and equipment. Occasional work on the Department of War (DoW) Secret Internet Router Network (SIPRNet) or Classified end user devices may be required. All tasks will be conducted in full compliance with DoW security regulations and DoW/Marine Corps cyber security policies. Designated personnel will have at a minimum, a "SECRET" security clearance. Contractors shall comply with the security requirements included in the Contract Security Classification Specification DD Form 254.

4.14.2 This requirement is limited to 1st tier subcontracting. The Contractor shall ensure it, and all subcontractors have completed the DD Form 254. All DD Form 254 requirements must be completed and approved prior to commencing any work under this contract. Before any subcontracting can take place, approval from the Government Cognizant Security Officer is required. If the Contractor substitutes a subcontractor, a revised DD Form 254 must be provided, and substitution can only take place once the Government Cognizant Security Officer approves the DD Form 254. The revised DD-254 shall be provided to the COR within 30 days from subcontractor change notification to the COR.

4.14.3 Personnel whose duties meet the criteria for an automated information system (AIS) Level 1 designation require a favorably adjudicated Tier 5 (T5) or Tier 5 Review (T5R) of the Single Scope Background Investigation (SSBI). This applies to all Information Assurance (IA) and Cybersecurity tasks. The T5 or T5R must be updated every 5 years. A favorably adjudicated Tier 3 (T3) or Tier 3 Reinvestigation (T3R) for Contractor personnel is required for AIS Levels 2 and 3. Additionally, National Telecommunications Directive (NTD) 02-06, Information Assurance (IA) Training Requirement, DoD 8140-M, Cyber Security Training, Certification, and Workforce Management Policy, and DoD 8500.2 E3.3.7 require that all authorized users of DoW Information Systems receive initial IA awareness orientation as a condition of access and thereafter must complete annual IA refresher awareness training to maintain an active user account. Access requests to DoW IT systems must utilize OPNAV 5239/14 (July 2008) SAAR-N form. SECNAVMAN 5239.2 IA Workforce Management Manual provides additional amplifying policy and requirements.

4.14.4 Communication Security (COMSEC): The data management and processing systems being managed include COMSEC equipment and material. The Contractor must meet COMSEC briefing and Local Element management certification requirements available under the OPNAVINST 2201.4, DoD Instruction 8523.01 and Air Force Manual 17-1301.

4.14.5 The Contractor must develop, implement and maintain an OPSEC program; pursuant to the National Security Decision Directive Number 298, DoD Directive 5205.2, USMC OPSEC guidance, and supplementary instructions. The Contractor's OPSEC program must be in accordance with this PWS and

DRAFT

the DD-254 Contract Security Classification Specification. Additionally, the Contractor's OPSEC program must comply with security requirements imposed by documents generated in response to DoD 5200.39, Critical Program Information (CPI) Protection within the DoW, July 16, 2008, as well as EDCOM's imposed OPSEC requirements. The Contractor must comply with DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. If a conflict is identified between USMC and higher-level guidance, the Contractor must contact the COR for clarification. Additionally, the Contractor's OPSEC program must enhance protection of classified and unclassified critical information, used at the Contractor's location. Subcontractors must also comply with all OPSEC requirements stated in this PWS.

4.14.6 The Contractor must coordinate OPSEC Awareness education and training through EDCOM. The COR can reasonably assist with training coordination. All personnel supporting the contract must receive initial OPSEC awareness training and annual OPSEC refresher training. The Contractor may use existing EDCOM's approved OPSEC awareness education, training, and planning processes vice creating a new program which will be provided at contract award.

4.14.7 The Contractor must provide the OPSEC plan to the COR no later than 60 days after contract award. Program protection measures must be applied and approved at all locations where Critical Information is developed, produced, analyzed, maintained, transported, stored, tested, or used in training. While performing on a government site, the Contractor must comply with the OPSEC guidance or plans specific to that location or program supported. The Contractor must request guidance from the COR on any specific predetermined OPSEC critical information.

4.14.8 Security Clearance and Mission Essential Personnel Matrix

The following table depicts the security clearance levels and mission essential contractor personnel required for each task area and requirement of the PWS, per description included in section 5 of the PWS.

Requirement	**PWS Section**	**Security Clearance Required**	**Mission Essential per DFARS 252.237-7023 and 7024**
Network and Systems Support	5.1.	Secret	Yes
Cybersecurity and Information Security	5.2.	Secret	Yes
Technical Support	5.3.	Secret	Yes
AV/VTC Support	5.4.	Secret	Yes

Facility Security Officers (FSOs) are responsible for notifying the Marine Corps University (MCU) Security Manager if any Contractor performing on this contract receives an unfavorable adjudication. The FSO must also notify the PERSEC Office of any adverse/derogatory information associated with the 13 Adjudicative Guidelines concerning any Contractor performing on this contract, regardless of whether a Defense Information System for Security (DISS) Incident Report is submitted. The FSO shall notify the Government (written notice) within twenty-four hours of any Contractor personnel added or removed from the contract that have been granted classified access, issued a Common Access Card (CAC) and/or any type of government building access badge that has been issued in the performance of this Contract.

DRAFT

Security Clearance Type	Vacancy Backfilling Timeline
Replacement of personnel requiring unclassified access	Within 30 days upon vacancy
Replacement of personnel requiring Secret	Within 60 days upon vacancy

4.15. Quality Assurance Plan (QAP). The Contractor shall provide a QAP that incorporates the contractor's quality control processes with the Government's terms and conditions for acceptance of products and services. The QAP will incorporate the Government's established requirements for acceptance of work, performance quality, and associated deliverables.

The Contractor shall develop and include a set of functional metrics at both the Division and task order level that shall serve as a means for performance benchmarking. Such metrics will be employed by the COR as a means for gauging overall effectiveness and correcting any problems associated with performance. Overall quality ratings will be provided to the Contractor quarterly for task order performance. The Contractor shall provide their QAP to the COR within thirty (30) days after contract award for review and comment.

4.16. Government-Furnished Property (GFP). The GFP, Material, Equipment, or Information Hardware and software upgrades and additions to networks and systems under the cognizance of EDCOM will be purchased by the Government before being furnished to the contractor for implementation at EDCOM. Government furnished information will include all applicable DoW/DON/USMC policy, guidance and direction for network systems administration and operation.

4.17. Certification Requirements. The table below outlines the certifications required of Contractor personnel supporting this contract per DoD 8140 DoD Cyber Workforce Framework (DCWF). No waivers or exceptions will be considered. The Contractor shall deliver copy of certifications of employees assigned to support this contract within 10 days after the task order award. Contractor shall ensure that employees maintain all applicable certifications current. After contract award, copies of certification status may be requested by the COR at any time during the task order performance and document must be provided within 5 days after request.

Requirement	DCWF Codes	Level	Minimum
System Engineering Support	451	Advanced	CompTIA CASP+ / SecurityX and Windows Server Hybrid Administrator Associate (AZ-800 & AZ-801)
Systems Administration	451	Intermediate	Security+ CE
Network Engineering Support	441	Advanced	CompTIA Security+ and Cisco Certified Network Professional (CCNP) Enterprise
Cloud Engineering Support	628	Advanced	CompTIA CASP+ / SecurityX and Azure Administrator Associate (AZ-104) or Azure Security Engineer Associate (AZ-500) or Azure Solutions Architect Expert (AZ-305)
Knowledge Management	431	Advanced	CompTIA CASP+ / SecurityX
Cable Management	442	Intermediate	CompTIA A+ or Network+

DRAFT

Technical Support	451	Intermediate	CompTIA Security+ CE, CompTIA Cloud+, SSCP, GSEC or GISCP
Cybersecurity Engineering Support	461/521/722	Advanced	ISC2 CISSP or CompTIA CASP+ / SecurityX
ATO Administration	722	Advanced	ISACA CISM or ISC2 CISSP
AV/VTC Support	411	Basic/Intermediate	CompTIA A+ CE, CompTIA Network+ CE or Security+ CE

4.18. Data Rights

4.18.1 General. The Contractor shall provide deliverables pursuant to the terms and conditions of this contract. In accordance with DFARS Clause 252.227-7989 (included in the contract) and other laws and regulations, all data, items, and materials, regardless of format, created, generated, produced, and associated intellectual property, that are required to be delivered or provided under, or as a result of, this contract (Items) shall become the property of (or licensed for unrestricted and perpetual use by) the U.S. Government, including but not limited to the Marine Corps; therefore, the U.S. Government/Marine Corps (also referred to as the "Government") shall have the irrevocable, royalty-free, worldwide right to use, modify, reproduce, perform, display, release, or disclose such Items, in whole or in part, in any manner, and for any purpose whatsoever, and to have or authorize others to do so. All Contractor-developed databases, analyses, evaluations, papers, training- or curriculum-related materials, studies, applications, and information completed or in progress under the contract are included as Items and shall be solely and fully owned by the Government. The Contractor shall turn over all contract-developed databases, analyses, studies, applications, information and other Items/Works, and all associated intellectual property, completed or in progress, to the Government, if not already delivered, upon contract completion, or when directed by the COR. The Items described herein, and any other items, are hereinafter referred to individually or collectively as the Work or Works. Specifically, the copyright and/or other intellectual property rights in or to the Works shall be assigned, and through execution of the Contract are assigned, or when appropriate licensed, to the U.S. Government/Marine Corps in accordance with DFARS Clause 252.227-7989.

4.18.1.1 To the extent the scope of U.S. Government/Marine Corps' use of third-party intellectual property rights may be dependent on contract/license terms the Contractor negotiates with third parties, the Contractor shall ensure such third-party contract/license terms provide the U.S. Government/Marine Corps all necessary rights and licenses to accomplish the Contract effort worldwide, including but not limited to providing the U.S. Government/Marine Corps with unrestricted and perpetual use of such license.

4.18.1.2 Compilation Works that include newly created and/or third-party intellectual property shall be assigned to the Marine Corps as a compilation Work.

4.18.1.3 The U.S. Government/Marine Corps shall have unrestricted access and use of all Deliverables upon delivery, and the U.S. Government/Marine Corps shall be provided with intellectual property rights of sufficient scope to allow unrestricted access and use of the data/materials, Items and Works, and other deliverables for future competitions or acquisitions. Moreover, the Contractor shall distribute data in the forms and quantities to the COR in accordance with the deliverables section of this contract.

DRAFT

4.18.1.4 The contract includes all applicable DFARS clauses to ensure protection and ownership of all technical data and other items generated. The Contractor shall provide all deliverables in a version, format, and media used/useable and modifiable by the U.S. Government/Marine Corps. For this effort, deliverables shall be provided in the format specified in the contract.

4.18.1.5 Unless intellectual property rights are licensed (in accordance with DFARS Clause 252.227-7989and approved by the KO) to provide all necessary rights and permissions to accomplish the effort/mission worldwide to the U.S. Government/Marine Corps, the U.S. Government/Marine Corps shall be the sole owner of all intellectual property and other rights in or to the Items/Works delivered under this contract. Therefore, any restricted data rights, information, software, materials and/or other items, including the Contractor's or a third-party's proprietary data, information, software, materials and/or items/Items, shall not be used under this Contract without the specific written approval by the KO prior to the start of any work that includes the use of any such restricted use items/Items/Works.

4.18.2 Management/Acquisition of Contractor and 3rd Party Software Licenses:

4.18.2.1 All software licenses the Contractor provides under this contract shall be transferable to the Government, shall not conflict with Federal law, and shall meet the Government's requirements under this contract. The Contractor shall obtain the Contracting Officer's concurrence prior to proceeding with any software and license acquisition in connection with this contract. Prior to the Contractor's (i) acquisition of any license to furnish the Government pursuant to this contract, or (ii) provision of any third-party license to the Government pursuant to this contract, the contractor shall submit the license to the Contracting Officer (CO) and Contracting Officer's Representative (COR) for review and acceptance. If the CO determines license provisions are inconsistent with Federal law and regulation, the Contractor shall negotiate changes with the software vendor at no additional cost to the Government. Thereafter, the Contractor shall submit the software and revised license to the CO and COR for review and acceptance prior to the delivery of the software and license to the Government. If the Contractor is unable to negotiate changes that are acceptable to the Government, the Contractor shall notify the CO and COR immediately.

4.18.2.2 Licenses or Terms and Agreements for third party software the Contractor acquires in connection with, or furnishes under, this contract shall not include the following:

4.18.2.3 Indemnification by the Government. *See* 31 USC § 1341.

4.18.2.3.1 Representation by any party of the United States or its Interests by any entity except the Department of Justice (DOJ). Only DOJ has authority to represent the United States or its interest in litigation, including but not limited to any Intellectual Property, Patent, and Copyright litigation concerning the Government. *See* 28 USC § 516.

4.18.2.3.2 Jurisdiction or venue outside United States Federal Courts or governing law that is not the laws of the United States of America. Any and all license terms and agreements shall be governed, interpreted and enforced in accordance with the laws of the United States of America. *See* 41 U.S.C. Chapter 41; FAR 52.212-4(e).

4.18.2.3.3 Binding arbitration.

4.18.2.3.4 Automatic renewal of the license. *See* 31 USC 1341.

4.18.2.3.5 Any order of precedence except for FAR 52.212-4(r).

DRAFT

4.18.2.3.6 Any Audit Clause except the following: "upon conclusion of the license and upon written request of the licensor, the government will provide a certificate of compliance duly executed by an official with authority to provide such certification."

4.18.2.3.7 Any warranty except for that provided in 52.212-4(o). The software shall be warrantied under 52.212-4(o) for a period of 180 days.

4.18.2.3.8 Termination rights belonging to the licensor or the Contractor that do not require prior consent of the Government.

4.18.3 Click licenses or click terms akin to those described in FAR 52.212-4(u).

4.18.3.1 Terms that do not comport with installation or mission requirements.

4.18.4 Embedded Third Party Software. The Contractor shall ensure any third-party software, and licenses applicable to such software, embedded in software the Contractor furnishes to the Government under this contract meet the terms set forth throughout this section. **Data Rights,** including but not limited to the submission of applicable license terms and software to the CO for review and concurrence.

4.18.4.1 All databases, analyses, evaluations, papers, training- or curriculum-related materials, studies, applications, information, programming code, instructions, reports, studies, Works, materials, Items, and anything else developed in regard to this contract are the property of the Government and may not be reused without prior written permission of the Government. Likewise, presentation of these Items/Works to the general public or any third party is prohibited without written permission of the Government.

4.18.5 Publicity and Marine Corps Brand. Neither the Contractor nor its subcontractors are authorized to use Marine Corps branding, copyrights, trademarks, or other intellectual property without prior written authorization from the CO.

4.18.6 The rights and remedies described herein shall not be exclusive and are in addition to other rights and remedies provided by law or elsewhere included in this contract.

4.18.7 This contract incorporates by reference the current version (including any applicable Class Deviation) of DFARS 252.227-2028, 252.227-7990, 252.227-7991, 252.227-7992, 252.227-7995, 252.227-7996, 252.240-7997, and 252.227-7989.

4.18.8 Compliance with this section is a material requirement of this contract.

4.19 Transition. The Contractor shall provide the services necessary to ensure a successful transition of services. Throughout the transition-in period & transition-out periods, it is essential to minimize interruptions or delays to work in progress that would impact the mission. The Contractor must facilitate the transfer of work control, processing, and assigning functions during the transition-in/transition-out periods.

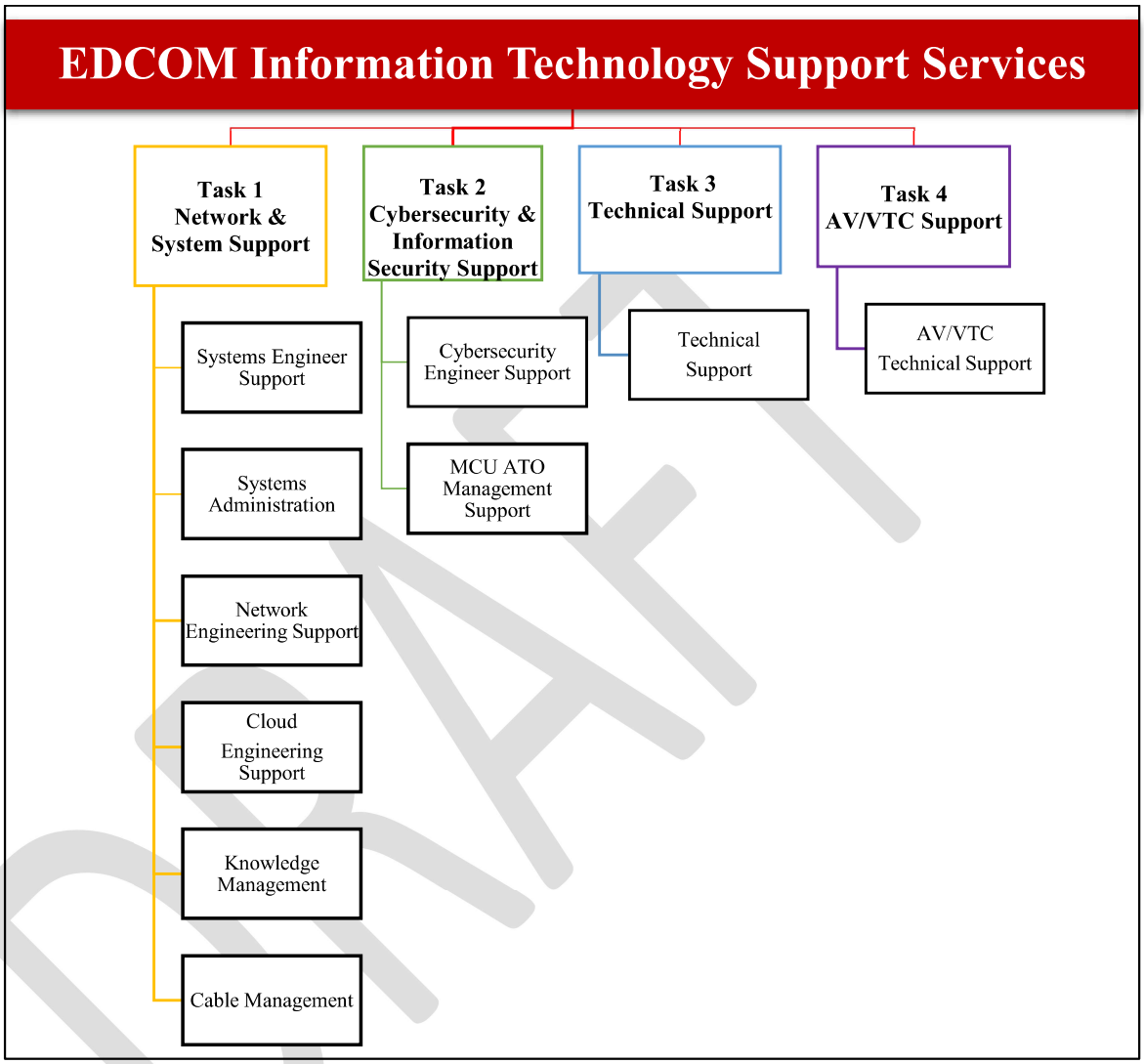
There will be up to a 30-day transition period, starting the day after award. The purpose of this transition-in period is to ensure a smooth transition of services from the predecessor contractor to the current contractor.

4.20 Contractor's Proposal Incorporation into Contract. The Contractor's proposal is hereby incorporated into the resultant contract and all subsequent task orders. In the event of conflict between the proposal and any other portion of the contract, the conflict shall be resolved in favor of the terms that were provided in the Government's proposal request. Moreover, if the contractor's proposal exceeds any PWS requirements it will become the minimum or threshold contract and task order requirement.

DRAFT

5. REQUIREMENTS.

The scope of this effort encompasses the following tasks and requirements:



5.1. <u>Task 1: Network and System Support.</u>

5.1.1. Requirement 1 – System Engineering Support

5.1.1.1. Configure, manage, monitor, report, troubleshoot, document and secure all required network services including but not limited to DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol, SNMP (Simple Network Management Protocol), HTTP / HTTPS (Web Services), SSH (Secure Shell), LDAP / LDAPS (Directory Services), SMTP (Simple Mail Transfer Protocol).

5.1.1.2. Update all servers, application software and network services in accordance with applicable Information Assurance Vulnerability Assessments (IAVAs), IAV Bulletins (IAVB), IAV Messages (IAVMs), Marine Corps Directives (MCDs), Operational Directives (OPDIRs) and CIO directives,

execute patches, and report compliance as required by Government established processes and deadlines.

5.1.1.3. Configure, manage, monitor, report, troubleshoot, document and secure EDCOM's Microsoft 365 productivity suite environment to include Outlook, Teams, Word, Excel, PowerPoint, SharePoint and OneDrive.

5.1.1.4. Configure, manage, monitor, report, troubleshoot, document and secure EDCOM's Microsoft Active Directory (AD) environment including but not limited to creating, testing, and linking Group Policy Objects (GPO), designing and maintaining the Organizational Unit (OU) structure to ensure that policies are applied to the correct units and groups, managing privileged account access by implementing Tiered Administration models (Tier 0, 1, and 2) management, managing the AD Schema; managing AD-Integrated DNS zones; configuring and reviewing "Advanced Audit Policy" settings and Trust management.

5.1.1.5. Configure, manage, monitor, report, troubleshoot, document and secure of EDCOM's Microsoft Configuration Manager (MCM) to include but not limited to operating deployment (imaging), software deployment, patching and upgrades, hardware and software inventorying and baselines, and Security Technical Implementation Guide (STIG) auditing and enforcement.

5.1.1.6. Design, configure, manage, monitor, troubleshoot, document, and secure the EDCOM VMware environment, encompassing ESXi hosts, vCenter servers, and all associated virtual infrastructure. This includes comprehensive lifecycle management, requiring the Contractor to execute virtual machine updates and upgrades, as well as managing snapshots and templates. To ensure continuous system integrity and strict compliance with DoW security mandates, the Contractor shall systematically apply all required security patches, bug fixes, and service packs.

To maintain optimal operations, services shall proactively track the health and performance of both virtual machines and physical hardware utilizing enterprise tools such as Azure Monitor and native VMware logs. The Contractor shall actively balance CPU, memory, and storage resources across the environment to prevent system bottlenecks. Furthermore, the Contractor shall develop and generate detailed reports on system operations and performance trends to predict future resource requirements and inform proactive capacity planning.

Diagnose and resolve complex technical anomalies, including virtual machine connectivity issues, storage latency, and host failures. This requires conducting thorough root cause analysis by examining critical system logs, including but not limited to vmkernel.log, hostd.log, and vpxa.log. Additionally, the Contractor shall rapidly troubleshoot and resolve virtual switch (vSwitch) misconfigurations, network packet errors, and storage connectivity disruptions across iSCSI, NFS, and Fibre Channel (FC) protocols.

Implement and enforce strict Role-Based Access Controls (RBAC) to restrict administrative access to authorized personnel only. The Contractor shall also configure virtual firewalls in continuous adherence to organizational security policies, applicable Security Technical Implementation Guides (STIGs), and industry best practices. Finally, the Contractor shall implement, manage, and support enterprise backup solutions and disaster recovery mechanisms. This requirement includes the regular testing, validation, and documentation of disaster recovery plans to guarantee the rapid restoration of mission-critical services following any operational disruption.

5.1.1.7. Design, configure, manage, monitor, troubleshoot, document, and secure the EDCOM Virtual Desktop Infrastructure (VDI) solution utilizing Azure Virtual Desktop (AVD). This includes the comprehensive management of AVD host pools, dynamically adding new session hosts to meet user demand, and configuring automated scaling plans to optimize virtual machine power states and maximize

DRAFT

cost efficiency. Create, maintain, and routinely update VDI "golden images" with the latest operating system patches and required business applications. Monitor and schedule all necessary updates for the AVD Agent across all deployed session hosts to maintain uninterrupted Azure service connectivity.

Configure and adjust Breadth-first or Depth-first load-balancing algorithms as needed to resolve performance bottlenecks or maximize host density. Manage the delivery of customized user environments by setting up, maintaining, and troubleshooting FSLogix profile containers. Additionally, manage AVD application groups to ensure users have secure, targeted access to required software resources based on their mission roles.

Monitor the health and efficiency of the VDI environment using Azure Virtual Desktop Insights to track connection success rates, user logon times, and overall session host performance. Investigate and resolve network latency or connection drops by auditing Network Security Group (NSG) rules and verifying proper virtual network (VNet) peering configurations. In the event of system anomalies, the Contractor shall execute rapid troubleshooting procedures, which include resetting RDP connections, validating virtual machine resource health, and redeploying session hosts that become degraded or unresponsive.

Implement strict access controls by assigning Role-Based Access Control (RBAC) roles and managing user permissions through Microsoft Entra ID to secure VDI access. Provide Tier II/III support to troubleshoot and resolve access issues, specifically including instances where Multi-Factor Authentication (MFA) or conditional access policies inadvertently block legitimate user sign-ins. Continuously monitor the directory synchronization between the on-premises Active Directory and the cloud environment to prevent identity conflicts and ensure seamless user authentication.

5.1.1.8. Install, configure, manage, monitor, report, troubleshoot, document and secure all physical and virtual servers.

5.1.1.9. Recommend virtualization strategies and upgrades to reduce physical footprint and energy costs and simplify support requirements for data center and end user workstations.

5.1.1.10. Create and update systems architecture documentation to provide a functional overview of the solution and directly maps technology capabilities and components to requirements.

5.1.1.11. Create and maintain standard operating procedures, work instructions and job aids to document government process and procedures.

5.1.1.12. Create detailed and accurate After-Action Reports to capture and describe outages, services interruptions, failures or incidents per government direction and processes to include the inclusion of lessons learned and recommendations.

5.1.1.13. Track and report End-of-Life (EoL) and End-of-Support (EoS) dates, warranty and support status and subscription and licenses expiration dates for all systems, software, operating systems, firmware, tools and subscriptions per government directed processes and formats.

5.1.1.14. Recommend data storage and backup strategies to meet future capacity and performance requirements and reduce the risk of data loss in case of device or media damage or failure. Prepare system engineering requirements documents and assist in the design and implementation of data storage and backup solutions.

5.1.1.15. Maintain a separate usmcu.edu Internet domain, internal intranet/local area network (LAN) and EDCOM Azure Cloud environment IAW DoWI 8550.01, to include VPN configuration/support, firewall

DRAFT

support, intrusion detection system (IDS) support, vulnerability scans, Internet protocol (IP) management, domain name server (DNS) management, and Spam/abuse management.

5.1.1.16. Provide technical and administrative support services, including installation, operation, documenting, and maintenance, for network systems and servers running EDCOM software, to include operating system software such as Microsoft Server 2012 and higher, Microsoft Windows 2010 and higher, Macintosh OSX-12 and higher, and Red Hat Linux 6.x and higher. Servers will all be physical and/or virtual. Virtual servers will all be in a VMWare vSphere 6.x or higher virtual environment.

5.1.1.17. Monitor data center and cloud performance to ensure efficient utilization of resources and to detect conditions requiring corrective action.

5.1.1.18. Troubleshoot hardware and software problems for hardware connected to the network and software running on servers or client workstations to problems, recommend solutions, and implement corrective actions.

5.1.1.19. Develop, configure, execute, secure and test data and system backup plans per Government provided processes and schedules.

5.1.1.20. Establish and maintain connections to proxy servers and other sites required to provide access to external databases and subscription services by authorized personnel.

5.1.1.21. Provide assistance in preparation of technical refresh plans for the data center and network to ensure that equipment and software is reliable. Upgrades to software and hardware on the network will be approved by the COR and will be installed by the Contractor. The Contractor will install Government-provided equipment, as approved by the COR, to upgrade existing infrastructure or add capacity and/or capabilities to the existing systems.

5.1.1.22. Validate and recommend changes, if required, to systems and services designs for planned expansion of existing EDCOM networks and data centers.

5.1.2. Requirement 2 – Systems Administration

5.1.2.1. Monitor, report, and assist in troubleshooting all required network services including but not limited to DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), NTP (Network Time Protocol, SNMP (Simple Network Management Protocol), HTTP / HTTPS (Web Services), SSH (Secure Shell), LDAP / LDAPS (Directory Services), SMTP (Simple Mail Transfer Protocol).

5.1.2.2. Assist the system engineer with updating all servers, application software and network services in accordance with applicable of Information Assurance Vulnerability Assessments (IAVAs), IAV Bulletins (IAVB), IAV Messages (IAVMs), Marine Corps Directives (MCDs), Operational Directives (OPDIRs) and CIO directives, execute patches, and report compliance as required by government established processes and deadlines.

5.1.2.3. Monitor, report, assist the system engineers troubleshoot EDCOM's Microsoft 365 productivity suite environment to include Outlook, Teams, Word, Excel, PowerPoint, SharePoint and OneDrive.

5.1.2.4. Assist troubleshooting EDCOM's Microsoft Configuration Manager (MCM) to include but not limited to operating deployment (imaging), software deployment, patching and upgrades, hardware and software inventorying and baselines, and STIG auditing and enforcement.

5.2.2.5. Assist with VMWare related tasks at remote sites.

5.1.2.6. Assist with Virtual Desktop Infrastructure (VDI) / Azure Virtual Desktop (AVD) related tasks at remote sites.

5.1.2.7. Assist with the installation, configuring, management, monitoring, reporting, troubleshooting, documenting and securing physical servers at remote sites.

5.1.2.8. Assist with creating and maintaining standard operating procedures, work instructions and job aids to document government process and procedures.

5.1.2.9. Assist with creating detailed and accurate After-Action Reports to capture and describe outages, services interruptions, failures or incidents per government direction and processes to include the inclusion of lessons learned and recommendations.

5.1.2.10. Assist with the tracking and reporting of End-of-Life (EoL) and End-of-Support (EoS) dates, warranty and support status and subscription and licenses expiration dates for all systems, software, operating systems, firmware, tools and subscriptions per government directed processes and formats.

5.1.2.11. Assist with troubleshooting hardware and software problems for hardware connected to the network and software running on servers or client workstations to problems, recommend solutions, and implement corrective actions at remote sites.

5.1.3. Requirement 3 – Network Engineering Support

5.1.3.1. Design, configure, manage, monitor, troubleshoot, report, document and secure EDCOM's Cisco based .edu Local Area Network (LAN) network to include but not limited to routing and switching configurations, routing protocols such as OSP, EIGRP, BGP and HSRP / VRRP, Access Control Lists (ACLs), site-to-site VPNs and tunnels, Virtual LANs (VLANs) and trunking, VRF (Virtual Routing & Forwarding), STP (Spanning Tree Protocol), Port Security, Quality of Service (QoS), IPSec, encryption protocols, TACACS+ / RADIUS , 802.1x, SSH, HTTPS/TLS, SNMPv3, NTP, DHCP, DNS, SysLog, NetFlow, bandwidth utilization and traffic patterns, packet capture and analysis, configuration backups and recovery, IOS and firmware upgrades, connections to the Azure Cloud (ExpressRoute or VPN) and the internet, centralized Authentication, Authorization, and Accounting (AAA), applying and verifying DISA STIGs, Cisco Security Advisories.

5.1.3.2. Design, configure, manage, monitor, troubleshoot, report, document and secure EDCOM's Cisco based wireless BYOD CampusNet network to include but not limited to wireless LAN controllers (WLCs), wireless access points (WAPs) enforcing WPA3-Enterprise or WPA2-AES encryption protocols on all SSIDs, Wireless Intrusion Detection/Prevention System (WIDS/WIPS) to detect and mitigate rogue access points, to ensure guest traffic never touches the internal LAN, RF site surveys (using tools like Ekahau) to identify coverage gaps, "dead zones," and high-interference areas, monitoring the RF spectrum for non-Wi-Fi interference (e.g., microwaves, Bluetooth, or malicious jammers), wireless heatmaps showing signal strength (RSSI) and Signal-to-Noise Ratio (SNR) for all floors/buildings, Co-Channel Interference, STIG and Access Point STIG Cisco AireOS or IOS-XE wireless images across the fleet of APs. Cisco DNA Center (DNAC) or Prime Infrastructure for centralized monitoring.

5.1.3.3. Create and manage Cisco Technical Assistance Center (TAC) tickets as required and report status to government personnel.

DRAFT

5.1.3.4. Develop, manage, report and document EDCOM's IP address Management (IPAM) and VLAN management.

5.1.3.5. Design, configure, manage, monitor, troubleshoot, report, document and secure EDCOM's network circuits and connections.

5.1.3.6. Design, configure, manage, monitor, troubleshoot, report, document and secure network access controls, administrative authentication and logging on both the .edu LAN and BYOD CampusNet wireless network via Cisco Secure Access Control System (ACS) or Cisco Identity Services Engine (ISE).

5.1.3.7. Coordinate with DISA or commercial providers for the installation, testing, and troubleshooting of WAN/Cloud circuits.

5.1.3.8. Create and update accurate physical and logical network diagrams (Visio) and rack elevations for the .edu LAN and BYOD CampusNet wireless network to include all supported EDCOM location.

5.1.3.9. Create and update systems architecture documentation to provide a functional overview of the solution and directly maps technology capabilities and components to requirements.

5.1.3.10. Create and maintain standard operating procedures, work instructions and job aids to document government process and procedures.

5.1.3.11. Create detailed and accurate After-Action Reports to capture and describe outages, services interruptions, failures or incidents per government direction and processes to include the inclusion of lessons learned and recommendations.

5.1.3.12. Track and report End-of-Life (EoL) and End-of-Support (EoS) dates, warranty and support status and subscription and licenses expiration dates for all LAN and wireless hardware, software, operating systems, firmware and tools per government directed processes and formats.

5.1.3.13. Support the Cisco RMA (Return Merit Authorization) and other hardware and software warranty actions in accordance with government direction and processes.

5.1.3.14. Install, move and cable LAN and wireless hardware such as physical routers, switches, WLCs, WAPs, within data centers and telecommunications closets (TRs) at all supported EDCOM locations in support of technical refresh projects and changes to EDCOM requirements.

5.1.3.15. Update all network devices to include routers, switches, wireless access points (WAPs), wireless LAN controllers (WLCs), applications, software, protocols and network services in accordance with applicable of Information Assurance Vulnerability Assessments (IAVAs), IAV Bulletins (IAVB), IAV Messages (IAVMs), Marine Corps Directives (MCDs), Operational Directives (OPDIRs) and CIO directives, execute patches, and report compliance as required by government established processes and deadlines.

5.1.3.16. Assist with addressing and solving system connectivity and failures to increase network uptime.

DRAFT

5.1.4. Requirement 4 – Cloud Engineering Support

5.1.4.1. Provide support for the engineering, deploying, and maintaining of a high-availability cloud infrastructure within EDCOM's Microsoft Azure Impact Level 2 (IL2) environment in order to ensure mission-critical applications and data are hosted in a secure, scalable, and resilient architecture that adheres to DoW Cloud Computing SRG (Security Requirements Guide) standards.

5.1.4.2. Configure and maintain Microsoft Entra ID (formerly Azure AD) for centralized identity management and access, including Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA) and PIM (Privileged Identity Management).

5.1.4.3. Maintain the network and EDCOM Azure Cloud environment in accordance with DoW and Marine Corps information assurance (IA) policies to satisfy accreditation requirements, including the creation and maintenance of required IA plans and documentation.

5.1.4.4. Implement and enforce DISA STIGs and monitor EDCOM's Azure IL2 security posture using Microsoft Defender for Cloud and Azure Sentinel.

5.1.4.5. Configure Virtual Networks (VNets), Network Security Groups (NSGs), and ExpressRoute/VPN connectivity between on-premises EDCOM facilities and Azure.
5.1.4.6. Utilize Azure Monitor and Log Analytics to track system performance and consumption patterns and conduct cost-optimization to recommend right-sizing resources to ensure efficient use of government funds.

5.1.4.7. Deploy and configure core Azure resources such as virtual machines (VMs), storage accounts, virtual networks, and databases.

5.1.4.8. Implement organization-wide policies using Azure Policy to ensure compliance and security standards.

5.1.4.9. Track system health, uptime, and resource usage using Azure Monitor and Log Analytics.

5.1.4.10. Diagnose and resolve cloud service issues, performance bottlenecks, and failed data pipelines.

5.1.4.11. Configuring and managing backups and site recovery solutions to ensure business continuity.

5.1.4.12. Regularly reviewing Azure Advisor recommendations for cost savings, reliability, and performance.

5.1.4.13. Create and update systems architecture documentation to provide a functional overview of the solution and directly maps technology capabilities and components to requirements.

5.1.4.14. Create and maintain standard operating procedures, work instructions and job aids to document Government process and procedures.

5.1.4.15. Create detailed and accurate After-Action Reports to capture and describe outages, services interruptions, failures or incidents per government direction and processes to include lessons learned and recommendations.

5.1.4.16. Track and report End-of-Life (EoL) and End-of-Support (EoS) dates, warranty and support status and subscription and licenses expiration dates for all systems, software, operating systems,

DRAFT

firmware, tools and subscriptions per government directed processes and formats.

5.1.5. Requirement 5 – Knowledge Management

5.1.5.1 Provide design and development support for EDCOM Microsoft 365 SharePoint pages on the .edu, Marine Corps Enterprise Network (MCEN) Non-classified Internet Protocol Router Network (NIPRNet) and SIPRNet networks to include site design, automated routing, workflows, dashboards, file storage and file sharing strategies, and access controls.

5.1.5.2. Provide web design, development support and access controls for all content hosted on the American Forces Public Information Management System (AFPIMS).

5.1.5.3. Ensure web content is accurate and up to date to include removal of outdated information, removing or repairing broken links and features and ensuring no PII/CUI or unauthorized information is posted.

5.1.5.4. Provide web content training to Government section and department content managers.

5.1.5.5. Recommend updates to policies, procedures, job aids and work instructions related to use of Microsoft 365 SharePoint.

5.1.5.6. Recommend updates to policies, procedures, job aids and work instructions related to use and updating of content and sites hosted on American Forces Public Information Management System (AFPIMS).

5.1.5.7. Provide support for Microsoft Power BI to enable the development, use, training and support of interactive visualizations to enhance data-driven decision making.

5.1.5.8. Provide support for Microsoft Powe Apps to enable the development, use, training and support of custom business applications that interact with SharePoint, SQL and Microsoft Dataverse.
5.1.5.9. Provide support for Microsoft Power Automate to enable the development, use, training and support to automate repetitive tasks and create seamless workflows between different applications such as routing a document through several managers for digital signatures, linking Microsoft 365 services with external apps like Salesforce, Trello, or Gmail through pre-built connectors.

5.1.6. Requirement 6 - Cable Management

5.1.6.1. Perform media termination by installing, terminating/splicing, managing, replacing, testing, troubleshooting, documenting copper (Cat6/6A) and fiber optic (single-mode/multi-mode) cabling.

5.1.6.2. Use of Fiber Tester and power meters to test signal strength, locate faults, and repair damaged fiber.

5.1.6.3. Use of Fluke, OTDRs (Optical Time Domain Reflectometers) or equivalent test equipment to test connectivity, speed, and signal integrity of twisted pair and fiber optic cables.

5.1.6.4. Install conduit, cable trays, ladder racks, J-hooks, patch panels, racks, and cabinets including proper bend radius and weight distribution to prevent signal degradation.
5.1.6.5. Implement "Cable Dressing" standards using hook-and-loop (Velcro) straps. (Note: Plastic zip-ties are generally prohibited in DoW data centers to prevent cable pinching).

DRAFT

5.1.6.6. Ensure cabling avoids proximity to power lines or unshielded devices that could leak signals through compromising emanations.

5.1.6.7. Apply DISA Infrastructure STIGs, ensuring that all unused ports are physically capped or disconnected and that racks are properly locked and alarmed.

5.1.6.8. Mark up "As-Built" drawings and update Microsoft Visio network diagrams and rack elevations to reflect physical changes in the data center and telecommunication closets.

5.1.6.9. Maintain a master "Cable Schedule" or database (like NetBox or ServiceNow) that tracks room to switchport to network drop mappings.

5.1.6.10. Apply machine-printed labels to every cable end, patch panel, and wall plate using the ANSI/TIA-606-C standard or specific Command SOPs (e.g., *Building-Room-Rack-Port*).

5.2. <u>Task 2: Cybersecurity and Information Security Support.</u>

5.2.1. Requirement 1- Cybersecurity Engineering Support

5.2.1.1 Advise the Information System Security Manager (ISSM) on all matters related to cybersecurity and information security.

5.2.1.2. Support the ISSM with the development of cybersecurity and information security policies, procedures, guidance, and best practices for compliance with Federal laws, regulations, guidelines, orders and directives to ensure EDCOM systems are secure and compliant.

5.2.1.3. Assist the MCU Information System Security Officer (ISSO).

5.2.1.4. Support the creation, submission, processing and tracking of System Authorization Access Requests (SAARs) requests via digital SAAR forms and the online AutoSAAR tool

5.2.1.5. Support the implementation of the Department of War's (DOW's) Zero Trust Strategy on all EDCOM networks and systems.

5.2.1.6. Support cybersecurity incident response, forensics and investigations in accordance with Government processes and procedures to ensure that actors and causes are identified, appropriate corrective actions are taken, and reports are filed in a timely manner.

5.2.1.7. Support the deployment, administration and configuration of Microsoft Defender in accordance with government processes, procedures, standards and directives to ensure comprehensive endpoint and server threat prevention, detection, and response.

5.2.1.8. Support change management and configuration management for proposed changes and modifications to Windows Defender, ACAS and other cybersecurity systems, configurations, signatures and settings to include submitting change control requests and attending scheduled Change Control Board (CCB) meetings.

5.2.1.9. Assist in the development of Cyber documentation for all systems, networks, and etc. to include reviewing, editing, and changing documents which include but is not limited to A&A packages, Standard Operating Procedures (SOPs), Tactics, Techniques, and Procedures (TTPs), Memorandum of Agreement (MOA), local policies and guidelines, and briefings for internal and external customers.

DRAFT

5.2.1.10 Support token issuance by performing duties as a MCEN NIPRNet and SIPRNet Trusted Agent (TA).
Support Mobile Device Management (MDM) and Mobile Application Management (MAM) via configuration of Microsoft Intune.

5.2.1.11. Support STIG implementations and checklists both manual and automated for devices, systems, services, software, applications, and programs.
Manage, respond to, update and report on all cybersecurity related trouble tickets.

5.2.1.12. Support implementation, auditing and reporting of Information Assurance Vulnerability Assessments (IAVAs), IAV Bulletins (IAVB), IAV Messages (IAVMs), Marine Corps Directives (MCDs), Operational Directives (OPDIRs) and CIO directive, execute patches, and report compliance as required.

5.2.1.13. Support identification, tracking, corrective action and reporting of all vulnerabilities using government provided tools such as Assured Compliance Assessment Solution (ACAS).

5.2.1.14. Support system and application upgrades to government provided tools such as Assured Compliance Assessment Solution (ACAS) and Microsoft Defender.

5.2.1.15. Support the deployment, administration and configuration of Microsoft Defender and Microsoft Sentinel in accordance with government processes, procedures, standards and directives to ensure comprehensive endpoint and server threat prevention, detection, and response.

5.2.1.16. Support change management and configuration management for proposed changes and modifications to Windows Defender, ACAS and other cybersecurity systems, configurations, signatures and settings to include submitting change control requests and attending scheduled Change Control Board (CCB) meetings.

5.2.1.17. Create and update systems architecture documentation to provide a functional overview of the solution and directly maps technology capabilities and components to requirements.

5.2.1.18. Create and maintain standard operating procedures, work instructions and job aids to document government process and procedures.

5.2.1.19. Create detailed and accurate After-Action Reports to capture and describe outages, services interruptions, failures or incidents per government direction and processes to include the inclusion of lessons learned and recommendations.

5.2.1.20. Track and report End-of-Life (EoL) and End-of-Support (EoS) dates, warranty and support status and subscription and licenses expiration dates for all systems, software, operating systems, firmware, tools and subscriptions per government directed processes and formats.

5.2.2. Requirement 2 –MCU's Authority to Operate (ATO) Management Support

5.2.2.1 Support the Defense Information Assurance Risk Management Framework (DIARMF) process, governed by DoDI 8510.01.

5.2.2.2. Support the creation, management and updating of all Enterprise Mission Assurance Support Service (eMASS) packages which may include the Authorization to Operate (ATO), Authorization to

DRAFT

Operate with Conditions, Interim Authority to Test (IATT), Interim Authority to Build (IATB) and the Authorization to Connect (ATC).

5.2.2.3. Support the creation, update, review and submission of required RMF documents to include but not limited to System Security Plans (SSPs), the Security Assessment Reports (SARs), the Plan of Action and Milestones (POA&Ms), Risk Assessment Reports (RARs), STIG Checklists, ACAS Scans, hardware and software baselines, and network and system diagrams.

5.2.2.4. Support the review, revision and update of EDCOM ATO packages and documents.
Support the identification, documentation, implementation, auditing and reporting of required security controls in accordance with NIST 800-53 and tailor them to the specific mission environment.

5.2.2.5 Complete government provided required DISA eMASS training and DoW RMF training courses within 30 days of contract award or hire date.

5.3. <u>Task 3: Technical Support.</u>

5.3.1. Requirement 1 – Technical Support

5.3.1.1. Provide support during core hours (currently Monday – Friday 0730 – 1700); however, weekend and after hours may be occasionally required due to mission requirements. Users may request support in person, by telephone, by e-mail or via Microsoft Teams.

5.3.1.3. Create, manage and resolve accurate and complete trouble tickets for all user reported issues and service requests.

5.3.1.4. Troubleshoot and resolve identified application and configuration problems via telephone assistance call, remote control, and at user locations, including but not limited to operating systems, software, authentication, printing, email, wired and wireless connectivity, M365 applications, etc.

5.3.1.5. Create, modify, maintain, delete, and troubleshoot Microsoft Active Directory user accounts and objects.

5.3.1.6. Support the creation, submission, processing and tracking of System Authorization Access Requests (SAARs) requests via digital SAAR forms and the online AutoSAAR tool.

5.3.1.7. Install and troubleshoot government provided Microsoft operating system images to government end user devices using Microsoft Configuration Manager (MCM).

5.3.1.8. Report verified or suspected Microsoft operating system image, software baseline and application issues to the government.

5.3.1.9. Install, configure, maintain and troubleshoot authorized client applications and software baselines on government end user devices using Microsoft Configuration Manager (MCM).

5.3.1.10. Support the deployment and testing of new client applications and software.

5.3.1.11. Apply configuration changes, service packs, patches, updates, security fixes and virus definition to government end user devices.

5.3.1.12. Support the administration, troubleshooting and user support for the Microsoft 365 productivity

DRAFT

suite to include Outlook, Teams, Word, Excel, PowerPoint, SharePoint and OneDrive.

5.3.1.13. Perform minor hardware troubleshooting, repair and replacements on government authorized computer systems such as hard drive replacements, memory upgrades, installing SLEP kits (Service Life Extension Program), etc.

5.3.1.14. Support hardware upgrades, replacements, moves and technical refresh projects to include moving, installing and cabling of government end user devices, monitors, phones, cell phones, wireless hotspots and other equipment.

5.3.1.15. Create, configure, maintain and trouble shoot printers and print services to include troubleshooting user reported printing, copying, scanning issues.

5.3.1.16. Support the management, issuance, configuration, tracking and troubleshooting of government cell phones and wireless hot spots and support loading Microsoft Intune and Microsoft 365 profiles to both government and personal cell phones.

5.3.1.17. Respond to standard trouble tickets within 24 hours from time issued, with a resolution within 48 to no more than 72 hours from trouble ticket creation.

5.3.1.18. Respond to command identified URGENT/VIP trouble tickets within 1 hour, with a resolution within 24 to 36 hours.

5.3.1.19. Report trouble ticket numbers, response time metrics and trends in the requested Government format at the quarterly program review meetings.

5.3.1.20. Submit and track the status of Telephone Service Requests (TSRs) to base telephone offices.

5.3.1.21. Report all confirmed or suspected cybersecurity incidents per established DOW, DISA, NAVI and USMC cybersecurity procedures.

5.3.1.22. Create and update work instructions, guides, job aids and process documents to document Government processes and procedures.

5.3.1.23. Support the Cybersecurity Branch with the collection of data and metrics related to security incidents as well as with the implementation of corrective action and application of security controls.

5.3.1.24. Support users with submitting Marine Corps Enterprise Network NIPR and SIPR trouble tickets via the Marine Corps Enterprise Service Desk.

5.3.2. Break/Fix: The Contractor shall provide break/fix technical support and perform minor hardware troubleshooting, repair, and component replacement to Government Furnished Equipment (GFE) and systems and provide critical items that could impact command operations such as hard drives, solid-state drives (SSDs), Random Access Memory (RAM), power supplies, batteries, graphics cards, cooling fans, card readers, network interface cards (NICs), transceivers, media converters and adapters, network cables, keyboards, mice, and monitors, KVM switches, web cameras, projector lamps/bulbs, AV cabling (HDMI, DisplayPort, Cat6 audio/video baluns), microphones, headsets, and like items. This requirement will not be used to procure new or replacement systems, provide new capabilities, or address new requirements.

DRAFT

5.4. <u>Task 4: Audiovisual and Video Teleconference (AV/VTC) Support.</u>

5.4.1. **Requirement 1- AV/VTC Technical Support:** The Contractor shall provide AV/VTC support to EDCOM.

5.4.1.1. Provide user level configuration, functionality and operation checks, AV/VTC system operation, status reporting, monitoring, inventorying, preventative maintenance, user level troubleshooting for AV/VTC equipment and systems.

5.4.1.2. Configure AV/VTC equipment for proper user operation and troubleshooting problems that occur before or during AV/VTC events, classes and meetings.

5.4.1.3. Operate complex audiovisual systems in auditoriums, lecture halls, classrooms and conference rooms in support of events, classes and meetings.

5.4.1.4. Operate auditorium production equipment such as lighting, camera, mics and recording equipment in support of events, classes and meetings.

5.4.1.5. Provide AV/VTC system operational support outside of normal working hours and have the capacity to surge support in times of event saturation.

5.4.1.6. Conduct scheduled operational checks of AV/VTC systems and equipment and report operational status per government direction.

5.4.1.7. Configure and troubleshoot problems with AV systems and associated computer equipment in classrooms.

5.4.1.8. Assist in the scheduling of events, classes and meetings involving the use of AV/VTC assets.

5.4.1.9. Instruct users in the proper operation of AV/VTC systems and perform physical equipment setup of auditoriums, lecture halls and classrooms, when required.

5.4.1.10. Possess knowledge of and experience in the operation of AV/VTC systems, for example Crestron, Extron and Cisco.

5.4.1.11. Respond to AV/VTC related customer trouble calls and support requests to include updating trouble tickets in the IT/AV ticket tracking software or system.

5.4.1.12. Support moving, replacing (swapping out), installing AV/VTC equipment in support of events, classes, meetings and tech refresh projects.

6. DELIVERABLES.

6.1 Deliverables are identified within the PWS and summarized in the table below. Execution of the PWS tasks will frequently yield deliverables in the form of, but not limited to, reports, papers, and presentation packages such as PowerPoint briefings, slides, and other PWS required deliverables. Reports shall contain information in sufficient detail to ensure that a professionally qualified third party can follow the logic of the report(s). The Government will provide written acceptance, comments, and/or change requests, if any, within five (5) business days from receipt of any formal deliverable. If written acceptance, comments, and/or change requests are not provided within five (5) business days, the deliverable shall be deemed acceptable as written by the contractor. If the Government provides comments and/or change requests, the

DRAFT

Contractor shall have five (5) business days from receipt of the Government correspondence to incorporate the comments and/or change requests and resubmit the deliverable. Formal quality control measures are expected to be executed for all formal deliverables. The table below shows the key deliverables and milestones the contractor shall be responsible for during the base year.

6.1.1 Specific Deliverables (unless otherwise directed by the COR the following sections describe the Specific Deliverables).

6.1.1.1 Monthly Status Report. The Contractor shall submit a Monthly Status Report to the COR, no later than the tenth (10th) calendar day of the following month for the work accomplished from the first (1st) through the final calendar day of the previous month. This report should be provided in electronic media and include the following information:

-Contract Number
-Period covered.
-Narratives describing task progress with reference to the specific PWS task (e.g., 5.2.1.) during the past month, plans for the forthcoming month, and any problems (actual or anticipated) requiring Government action. For identified (actual) problems, the Contractor shall state the impact in terms of work completion dates, as well as provide a plan for correction.
-COR approved deliverables submitted.
-Travel costs, including trip reports, purpose of trips, duration, and related actions.
-Personnel turnover and future staffing projections.
-Objectives for the upcoming month.
-Any issues either current or anticipated with recommended solutions.
-Amendments to the reporting format may be directed by the COR.

6.2. Deliverables

Deliverable Name / Title	Associated PWS Task(s)	Description	Frequency / Milestone
Quarterly Meeting Minutes	4.13	Delivery of meeting minutes of Quarterly Performance Review Conferences. Minutes shall include fate, name of attendees and excerpt of discussion.	Quarterly meetings minutes to be submitted to the COR within 5 business days.
Revised DD-254	4.14.2	Accurate and timely delivery of Contract Security Classification Specification DD Form 254 to account for changes in team members.	Revised DD-254 to be delivered no later than 30 days from subcontractor change notification to the COR.
OPSEC Plan	4.14.7	OPSEC plan	Delivery to the COR no later than 60 days after contract award.

DRAFT

Quality Assurance Plan (QAP)	4.15.	The Contractor shall provide a QAP that incorporates the contractor's quality control processes with the Government's terms and conditions for acceptance of products and services. The QAP will establish the requirements for acceptance of work, performance quality, and associated deliverables. The Contractor shall develop and include a set of functional metrics at both the Division and task order level that shall serve as a means for performance benchmarking. Such metrics will be employed by the COR as a means for gauging overall effectiveness and correcting any problems associated with performance. Overall quality ratings will be provided to the Contractor quarterly for task order performance.	Delivery to the COR within ten (10) days after contract award.
Monthly Status Report	6.1.2.1	The Contractor shall submit a Monthly Status Report to the COR, no later than the tenth (10th) calendar day of the following month for the work accomplished from the first (1st) through the final calendar day of the previous month. This report should be provided in electronic media and include the following information: -Contract Number -Period covered. -Narratives describing task progress with reference to the specific PWS task (e.g., 5.2.1.) during the past month, plans for the forthcoming month, and any problems (actual or anticipated) requiring Government action. For identified (actual) problems, the Contractor shall state the impact in terms of work completion dates, as well as provide a plan for correction. -COR approved deliverables submitted. -Travel costs, including trip reports, purpose of trips, duration, and related actions. -Personnel turnover and future staffing projections. -Objectives for the upcoming month. -Any issues either current or anticipated with recommended solutions. -Amendments to the reporting format may be directed by the COR.	Monthly.
System Architecture & Network Diagrams	5.1.1.10, 5.1.3.8, 5.1.3.9, 5.1.4.13, 5.1.6.8, 5.2.1.17	Comprehensive Visio diagrams, physical/logical topologies, "As-Built" drawings, and rack elevations mapping capabilities to requirements.	Review and provide recommendations within 60 days of contract start; drafts provided within 15 days, and final versions provided within 30 days for any architectural change.
Asset & Lifecycle Tracking Report	5.1.1.13, 5.1.2.10, 5.1.3.12, 5.1.4.16, 5.2.1.20	Database or tracker of End-of-Life (EoL), End-of-Support (EoS), warranty status, and license expirations for all hardware and software.	Quarterly.

DRAFT

Vulnerability & Patch Compliance Report	5.1.1.2, 5.2.1.11, 5.2.1.12, 5.2.1.13	ACAS scan results, STIG Viewer checklists, and compliance status for IAVAs, IAVBs, MCDs, and OPDIRs.	Monthly, and within 24-48 hours for URGENT/Critical OPDIRs.
After-Action Reports (AARs) & Incident Reports	5.1.1.12, 5.1.2.9, 5.1.3.11, 5.1.4.15, 5.2.1.6, 5.2.1.19, 5.3.1.21	Detailed documentation of outages, service interruptions, cybersecurity incidents, lessons learned, and recommended corrective actions.	Within 24-48 hours of incident resolution.
RMF & eMASS Authorization Artifacts	5.2.2.2, 5.2.2.3, 5.2.1.9	System Security Plans (SSPs), Security Assessment Reports (SARs), Risk Assessment Reports (RARs), ATO/IATT/ATC packages, hardware/software baselines.	Annually for major review; Continuous updates in eMASS as systems change.
Plan of Action and Milestones (POA&M)	5.2.2.3	Tracking matrix for all unmitigated cyber vulnerabilities, outlining mitigation strategies and target resolution dates.	Monthly update to the ISSM.
Standard Operating Procedures (SOPs) & TTPs	5.1.1.11, 5.1.3.10, 5.1.4.14, 5.1.5.5, 5.2.1.9, 5.3.1.22	Work instructions, job aids, MOAs, and Tactics, Techniques, and Procedures (TTPs) covering IT/Cyber operations and M365/SharePoint management.	Review and provide recommendations within 60 days of contract start; Updated annually or upon process change.
IT Helpdesk & Performance Metrics Report	5.3.1.19	Summary of trouble ticket volumes, response/resolution time metrics, SLA compliance, and trend analysis.	Insert in the Monthly Status Report.
Backup, Disaster Recovery & Storage Strategy	5.1.1.14, 5.1.1.19	Engineering requirements document outlining data storage strategies, system backup plans, and DR testing schedules.	Review and provide recommendations within 60 days of contract start; with bi-annual testing, exercising and updates.
Tech Refresh & Capacity Plans	5.1.1.9, 5.1.1.21, 5.1.4.6	Reports detailing hardware replacement schedules, cloud resource right-sizing (cost-optimization), and virtualization strategies.	Review and provide recommendations within 180 days of contract start; with bi-annual review and updates.
Cable Management Schedule	5.1.6.9, 5.1.6.10	Master database (e.g., NetBox) mapping rooms to switchports to network drops, conforming to ANSI/TIA-606-C standards.	Maintained continuously; audited Quarterly.
AV/VTC System Operational Status Report	5.4.1.6	Results of scheduled operational checks, preventative maintenance logs, and readiness status of auditorium/classroom systems.	Monthly.

8. PERFORMANCE REQUIREMENT SUMMARY.

8.1. The Performance Requirements Summary (PRS) table provided below identifies the mission critical items for performance under this contract. Only performance deficiencies that are directly attributable to Contractor error are considered when measured against the performance threshold:

PWS Reference	Performance Metric	Performance Level (Target)	Acceptable Quality Level (AQL)	Method of Surveillance
4.1 through 4.20	Compliance with all general PWS requirement	100% compliance	No more than 2 intents to resolve issues.	Meetings, Inspection, document reviews.
Task 1	**Network and System Support**			

5.1.1.2, 5.1.2.2, 5.1.3.15	Vulnerability Management & Patching: Apply IAVAs, IAVBs, MCDs, OPDIRs, and STIGs to all servers, network devices, and software.	100% compliance with DoW/USMC mandated deadlines for critical and high vulnerabilities.	95% of patches applied on time; remaining 5% mitigated with approved Plan of Action and Milestones (POA&M). Zero unmitigated critical vulnerabilities.	ACAS / Nessus Vulnerability Scans; STIG Viewer checklists; Monthly compliance reports.
5.1.1.1 - 5.1.1.8, 5.1.3.1 - 5.1.3.2	System & Network Availability: Maintain uptime for M365, AD, VMWare, VDI, and Cisco LAN/WLAN environments.	99.9% uptime for core network and infrastructure services during normal business hours.	99% uptime for core services. Maximum of 4 hours unplanned downtime per month per system.	Automated Network Monitoring Tools (e.g., SolarWinds, Cisco DNA Center); Azure Monitor; vCenter logs.
5.1.1.19, 5.1.4.11	Data Backup & Disaster Recovery: Execute and test system backup plans and site recovery solutions.	100% successful routine backups. Disasters/outages recovered within defined Recovery Time Objectives (RTO).	98% successful backups on the first attempt. Failed backups remediated and rerun successfully within 24 hours.	Backup software logs (e.g., Veeam); Azure Site Recovery logs; Quarterly failover/recovery test reports.
5.1.1.10 - 5.1.1.13, 5.1.3.8 - 5.1.3.12	Documentation & Reporting: Accurate AARs, Visio diagrams, SOPs, and EoL/EoS tracking databases.	100% accuracy of network diagrams, SOPs, and asset trackers. AARs submitted within 24 hours of incident resolution.	Updates to architecture/diagrams completed within 5 business days of a network change. 95% of AARs submitted on time.	Periodic Inspection by Contracting Officer's Representative (COR); ServiceNow/ITSM ticket audits.
5.1.2.11, 5.1.3.16, 5.1.4.10	Incident Resolution & Troubleshooting: Resolve hardware/software, cloud, and remote site connectivity issues.	100% of trouble tickets resolved within priority-based Service Level Agreement (SLA) timeframes.	90% of routine tickets resolved within standard SLA. 95% of urgent/mission-critical tickets resolved within SLA.	Helpdesk / ITSM system metrics and SLA reports; Customer feedback.
5.1.4.1 - 5.1.4.8	Cloud Security & Optimization: Manage Azure IL2 environment, Entra ID RBAC/MFA, and resource cost-optimization.	100% adherence to DoW Cloud Computing SRG and zero unauthorized access incidents. Continuous cost optimization.	Zero security breaches. Monthly Azure Advisor reviews conducted, and optimization recommendations implemented within 15 days.	Microsoft Defender for Cloud score; Azure Sentinel logs; Monthly Azure Billing/Utilization reports.
5.1.5.1 - 5.1.5.6	Knowledge Management & Content Accuracy: Support SharePoint and AFPIMS; ensure accurate, up-to-date content free of PII/CUI.	100% functional sites with zero broken links and absolute zero unauthorized PII/CUI spills.	Zero PII/CUI data spills (Strict AQL). Broken links or outdated content corrected within 48 hours of notification.	100% Inspection of flagged content; Automated link-checking scripts; User complaints.
5.1.6.1 - 5.1.6.10	Cable Management & Infrastructure Security: Install, terminate, test, and dress cables. Cap unused ports and maintain ANSI/TIA-606-C labeling.	100% of cabling installed securely (no zip-ties, proper dressing) and labeled perfectly. All unused ports capped per DISA STIG.	95% first-pass inspection rate for labeling and dressing. Corrective actions completed within 2 business days of COR notification.	100% Physical Inspection by COR/QA personnel; Fluke/OTDR test result reports; NetBox/Cable Schedule review.
Task 2	**Cybersecurity and Information Security Support**			

5.2.2.1 - 5.2.2.4	RMF & eMASS Administration: Maintain and update eMASS packages (ATO, IATT, IATB, ATC) and associated documents (SSP, SAR, POA&M, RAR).	Continuous authorization maintained. 100% compliance with DoWI 8510.01 RMF requirements and NIST 800-53 controls.	Zero lapsed authorizations (ATOs) due to contractor delay. POA&Ms updated monthly. 95% of eMASS artifacts submitted without rework.	ISSM Inspection of eMASS records; Monthly POA&M audits; DCSA/DoW cyber readiness inspections.
5.2.1.11 - 5.2.1.14	Vulnerability & Compliance Management: Execute ACAS scans, apply IAVAs/MCDs, and implement STIG checklists for all systems.	100% compliance with DoW mandated deadlines for vulnerability patching and STIG remediation.	95% compliance on standard deadlines; 100% compliance on critical OPDIRs/IAVAs. 100% of assets scanned by ACAS monthly.	ACAS / Nessus scan results; STIG Viewer checklists; Continuous Monitoring (ConMon) reports.
5.2.1.6, 5.2.1.7, 5.2.1.15, 5.2.1.19	Threat Detection & Incident Response: Administer Microsoft Defender/Sentinel and conduct incident response/forensics.	100% detection coverage on endpoints and servers. Immediate containment and reporting of cyber incidents.	Zero catastrophic network compromises due to misconfigured Defender/Sentinel policies. AARs submitted within 24 hours of incident closure.	Microsoft Sentinel dashboard alerts; Cybersecurity Incident Response Team (CSIRT) logs; AAR reviews.
5.2.1.4, 5.2.1.10	Identity & Access Management: Process SAARs (AutoSAAR), manage Microsoft Intune (MDM/MAM), and perform NIPR/SIPR Trusted Agent (TA) duties.	100% accurate token issuance and SAAR processing. All mobile devices compliant with Intune policies.	95% of SAARs and token requests processed within 2 business days. Zero unauthorized tokens issued (Strict AQL).	AutoSAAR system metrics; TA token issuance audit logs; Intune compliance dashboards.
5.2.1.8, 5.2.1.9, 5.2.1.16 - 5.2.1.18, 5.2.1.20	Cyber Documentation & Change Management: Create/update SOPs, TTPs, MOAs, architecture diagrams, and represent cyber at CCB.	100% accurate documentation and tracking of EoL/EoS dates. All cyber changes processed through formalized CCB.	Architecture and SOPs updated within 5 days of major system changes. Zero unapproved changes pushed to production.	CCB meeting minutes; Periodic documentation spot-checks by ISSM/COR; ServiceNow change logs.
5.2.1.1, 5.2.1.2, 5.2.1.3, 5.2.1.5	ISSM Support & Zero Trust: Perform ISSO duties, advise ISSM, and support DoW Zero Trust Strategy implementation.	Seamless integration of Zero Trust pillars and full operational support to the ISSM.	Consistent and proactive policy guidance provided. Zero major audit findings related to ISSO duties.	ISSM subjective review; Annual Cyber Readiness Inspection (CCRI) results.
5.2.2.5	Training & Qualifications: Complete required DISA eMASS and DoW RMF training courses.	100% of required ATO Administrators fully trained and certified in eMASS and RMF.	Personnel complete required training within 30 days of onboarding and maintain continuous certification.	DoW Cyber Workforce Management Program (CWMP) records; Training certificates
Task 3	**Technical Support**			
5.3.1.2	Desktop Computing Availability: Ensure users have access to all desktop computing functions (excluding external factors).	98% availability of all desktop functions during normal working hours.	98% uptime. Any deviation requires immediate user notification and progress updates.	Network monitoring tools; User availability reports; Customer feedback surveys.

5.3.1.17	Standard Trouble Ticket Response & Resolution: Time from ticket creation to initial response and final closure for routine issues.	Response: < 24 hours. Resolution: 48 – 72 hours.	95% of standard tickets resolved within the 72-hour window.	ITSM / Trouble Ticket system reports (e.g., ServiceNow, Remedy); Monthly Program Reviews.
5.3.1.18	Urgent / VIP Ticket Response & Resolution: Time from ticket creation to initial response and final closure for Command-identified priorities.	Response: < 1 hour. Resolution: 24 – 36 hours.	98% of Urgent/VIP tickets resolved within the 36-hour window.	Real-time ticket tracking; Daily status reports; COR feedback.
5.3.1.5, 5.3.1.6, 5.3.1.16	Account & Access Management: Manage AD objects, SAAR/AutoSAAR processing, and mobile device/hotspot configuration (Intune).	100% accuracy in AD object management and mobile profile deployment.	95% accuracy. 100% compliance with security protocols for SAAR/AutoSAAR processing.	AD audit logs; AutoSAAR tracking logs; Intune compliance dashboards.
5.3.1.7 - 5.3.1.11	Endpoint Configuration & Patching: Install/troubleshoot OS images, software baselines, and security patches via MCM.	100% of end-user devices updated with the latest approved patches, images, and virus definitions.	95% of devices compliant with current software baselines and patch levels within 5 days of release.	MCM (SCCM) compliance reports; ACAS vulnerability scans.
5.3.1.13 - 5.3.1.15	Hardware & Lifecycle Support: Minor repairs, tech refresh (moves/installs), and printer/scanner troubleshooting.	100% of authorized hardware upgrades and moves completed per schedule.	90% completion rate of tech refresh projects within the agreed-upon project timeline.	Asset management records; Monthly move/add/change (MAC) logs.
5.3.1.19, 5.3.1.22	Administrative Reporting & Documentation: Submit monthly metric reports and maintain SOPs/Work Instructions.	100% accurate and on-time submission of monthly program review metrics and trend analysis.	95% on-time submission of reports. Documentation updated within 10 business days of a process change.	COR review of monthly reports; Document version control audits.
5.3.1.21, 5.3.1.23	Cyber Incident Reporting: Detect and report confirmed or suspected cybersecurity incidents.	Immediate reporting of all suspected incidents per established DoW/USMC procedures.	100% compliance (Strict AQL). Zero failures to report suspected incidents.	
Task 4	**AV/VTC Support**			
5.4.1.2 - 5.4.1.5, 5.4.1.7	Live Event & Meeting Support: Configure, operate, and troubleshoot AV/VTC systems (e.g., Crestron, Extron, Cisco) and production equipment for scheduled classes and events, including surge/after-hours support.	100% of scheduled events, classes, and VTCs start on time without contractor-caused technical delays.	95% of events start flawlessly. Any pre-event or mid-event technical issues are resolved or mitigated within 5-10 minutes to minimize disruption.	Customer feedback; COR observation; Event/Meeting AARs.

5.4.1.1, 5.4.1.6	Preventative Maintenance & Checks: Conduct scheduled operational checks, preventative maintenance, and status reporting on all AV/VTC equipment.	100% of scheduled operational checks and preventative maintenance tasks completed per government schedule.	95% of routine checks completed on time. System operational status reports submitted accurately and on time per government direction.	Review of Preventative Maintenance (PM) logs; Status report audits.
5.4.1.11	Trouble Ticket Resolution: Respond to and resolve AV/VTC related customer trouble calls and update the IT/AV ticket tracking software.	100% of trouble tickets documented and resolved within established facility SLAs.	95% of standard AV/VTC tickets resolved within standard SLAs. 100% of tickets accurately logged in the tracking system.	ITSM/Ticket tracking system reports; Helpdesk metrics.
5.4.1.8, 5.4.1.9	User Instruction, Scheduling & Physical Setup: Assist with scheduling, perform physical room setups, and instruct users on proper system operation.	Complete 100% of requested physical setups accurately prior to event start and provide clear user instructions.	98% user satisfaction rate regarding physical room readiness and quality of user instruction provided.	Customer satisfaction surveys; Periodic spot checks by COR.
5.4.1.12	Equipment Lifecycle & Tech Refresh: Support moving, replacing, and installing AV/VTC equipment for events, classes, and tech refresh projects.	100% safe and accurate physical handling, installation, and inventory tracking of AV/VTC assets.	95% of installation/move projects completed within scheduled timelines. 100% accountability of all moved or replaced assets.	Property/Asset management audits; Post-installation COR inspection.

DRAFT