Department of Defense
Defense Health Agency
Performance Work Statement

Network Engineers and Specialists Support (NE&S)

Network Modernization Branch (NMB)

LAN Sustainment Section

Version: 1.0
Date: 07/09/2025

PART 1
1.0 GENERAL INFORMATION

1.1 This is a non-personal services contract to provide the Defense Health Agency (DHA) Network Modernization Branch (NMB) as defined in the Performance Requirements Summary (PRS) (Part 7, Attachment 1) of this PWS with Enteprise and MTF local site information technology (IT) support, and touch labor and to transition all DHA sites listed in this PWS to a fully integrated site and enterprise IT support Integrator (EITSI) SUPPORT MODEL.

1.2 Description of services/introduction: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform local IT support, and touch labor and to transition all DHA sites to a fully integrated site and Enterprise IT Services (EITS) support model EITSI as defined in this Performance Work Statement (PWS) except for those items specified as government furnished property and services. The contractor shall perform to the standards in this PWS.

As required by the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2017 and as amended in the FY 2019 NDAA, Authority, Direction, and Control (ADC) of all DoD Military Medical Treatment Facilities (MTFs) and Other Lines of Business (OLBs) will transition to the Defense Health Agency (DHA). This transition will enable tighter integration of healthcare delivery systems to achieve medical readiness, improve health of people, enhance experience of care, and lower healthcare costs.

As a result, the DHA established the Enterprise Information Technology Services (EITS) as a multi-provider, integrated environment for the delivery of IT services to the DHA and Military Health System (MHS). The mission of the EITS Program is to transform MHS IT through a services integration approach that standardizes service delivery, increases efficiency, and measures and improves quality. This new operating model will be implemented through the aggregation of IT delivery, management, and governance activities that allow for more efficient service delivery, timely decisions, and continuous improvement. The MHS EITS strategy includes three major components: EITS Integrator (EITSI), Capability Service Providers (CSPs), and Geographic Service Providers (GSPs).

- EITSI contractor specializes in coordination, integration, and management activities and will replace certain existing Enterprise contracts, including the DHA Global Service Center (GSC).
- GSPs are contractors that perform a wide variety of IT tasks and services for MTFs/OLBs spanning a defined geographic area.
- Capability Service Providers (CSPs) are specialist contractors that perform a particular IT capability and provide it to the entire MHS Enterprise.

This integrated environment will use a Multisourcing Services Integrator (MSI) approach to coordinate delivery across multiple IT contracts and service owners. This approach optimizes centralized control by assigning coordination, integration, and management activities to an

integrator function that specializes in these capabilities. It enables the reduction of site-specific solutions and increases capabilities of centrally-managed IT services.

The environment requires coordination, cooperation, communication, and integration amongst various participating entities. To accomplish this, the EITSI is the single contractor responsible for supporting and coordinating service delivery across the EITS environment. The EITSI has a distinct and separate role in coordinating with the other service providers. It will implement common business processes and tools for the delivery of IT services across the MHS. In addition, the EITSI will integrate with other contractors focused on their own service areas. Contractors with specialist focus in a particular enterprise service are referred to as CSPs and contractors performing IT support tasks at MTFs and OLBs spanning a defined geographical area are referred to as Geographic Service Providers (GSPs). The EITSI will also work with the existing incumbent contractors in the environment, even prior to their full integration. Specific scope of individual CSPs is still being defined by DHA. Integrated Service Providers will each have obligations in their contracts to interface with enterprise tools and processes

1.3 Background: The DHA mission is to plan, program, acquire, implement and sustain peacetime information technology infrastructure, and to train personnel and provide support services for the Military Health System (MHS) centrally managed products to improve and maintain the health of the MHS beneficiaries. Military health care delivery is heavily dependent upon automated information systems (AISs) which rely on a robust network infrastructure to transport data within and between Medical Treatment Facilities (MTFs). Numerous medical and administrative systems use the network including: MHS GENESIS, Defense Medical Logistics Standard Support (DMLSS), Defense Blood Standard System (DBSS), Expense Assignment System (EAS) IV, as well as various office automation and electronic mail systems, suites, and clinical software add-ons. The protocols and technologies that are present on the MTF LANs and interconnecting WAN are described in Attachment 1

1.4 Objectives: . The objective of this tasking is for the contractor to provide network (i.e. local, wireless, and wide area network) sustainment and deployment support services to the MHS MTFs, which includes hospitals, clinics, and other remote elements throughout CONUS and OCONUS locations. The Contractor shall, in the performance of this task order, be successful at coordinating and working with other vendors and Government agencies in resolving problems, gathering information, and/or making recommendations to the Government

1.5 Scope: On behalf of the DHA, this awarded task order will provide network sustainment and deployment support services to the MHS MTFs both inside and outside the continental United States (CONUS and OCONUS). This work includes functions such as network performance measurement and monitoring, assistance with network design and development, network measurement, customer service in the form of trouble tracking and troubleshooting at the Tier 0 level, onsite support for both contractor and Government support teams for escalated trouble tickets, as well as maintenance and sparing support in concert with DHA Asset Management & Support Services (AMSS). Such services will be provided in accordance with stated MHS and specific Medical Component priorities. Services shall also comply with existing and evolving technical architecture guidance from international, commercial, Department of Defense (DoD), and Health Affairs (HA) sources. These services will be provided in a

centralized and decentralized mode. The on-site network specialists will be the primary 24/7 on-call decentralized points of contact within the MTFs for all network related support as required for normal operations of the MTF and related facilities. Additional support and guidance will be provided by regional (i.e. CONUS, Asia and Europe) network engineers and the DHA centralized infrastructure team. The Government reserves the right to change this distribution to support mission criticality.

1.6 Period of Performance (PoP): One (1) 6-Month Base Period, inclusive of Transition, Four (4) 12-Month Option Periods, and an Option to Extend Services for up to six months IAW FAR 52.217-8 at the discretion of the Government.

1.6.1 **Transition**: Transition-in/transition-out period.

1.6.1.1 **Transition-in period**: Full performance start date is, 30 days (CONUS) or 45 days (OCONUS) from the first day of the period of performance. During the transition-in period, the contractor shall prepare to meet all contract requirements and ensure incoming personnel are functionally trained and qualified on the full performance start date except cybersecurity requirements, which must be fully adhered during transition and full performance periods. The remaining incoming personnel shall be trained and qualified within 30 days from the first day of the period of performance start date.

In accordance with the solicitation, the Contractor shall provide a plan for 30 days incoming transition from contract to contract. The Contractor shall coordinate with the Government in planning and implementing a complete transition to the Contractor's support model. The Contractor shall collaborate with the Government to develop and deliver an Incoming Transition Plan, CDRL A002 Transtion-in, Transition-out). The Government will designate a transition period for the incoming Contractor to coordinate and work with the incumbent Contractor. This transition plan shall include, but is not limited to:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new Contractor system
- Government-approved training and certification process
- Transfer of hardware warranties and software licenses (if applicable)
- Transfer of all necessary business and/or technical documentation
- Transfer of compiled and un-compiled source code, to include all versions, maintenance updates and patches (if applicable)
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes
- Distribution of Contractor purchased Government owned assets, including facilities, equipment, furniture, phone lines, computer equipment, etc.
- GFE inventory management assistance

Transfer and documentation of the receipt of Government Furnished Equipment (GFE) and Government Furnished Information (GFI) such as:

- Hardware/software
- Laptops/PCs
- Pagers/cell phones/calling cards
- Data/databases
- Common Access Cards (CAC)
- Procedural manuals/guidelines
- Operating instructions
- Historical data, e.g., memos, letters, correspondence, regulations, reports, documents and contract document library
- Agreement documents, e.g., software licensing agreements

The contractor shall comply with transition-in requirements of the DHA, as listed in paragraph 1.11.1, for contractors needing to be issued Common Access Card (CAC) identification, including Department of Defense (DoD) and DHA-directed training and forms submission, prior to network access.

1.6.1.2 **Transition-out period**: The transition-out plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the contract. See Part 7, Technical Exhibit 1.

This shall include formal coordination with Government staff and successor staff and management. It shall also include delivery of copies of existing policies and procedures, and delivery of required metrics and statistics. This transition plan shall include, but is not limited to:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new Contractor system
- Government-approved training and certification process
- Transfer of hardware warranties and software licenses (if applicable)
- Transfer of all necessary business and/or technical documentation
- Transfer of compiled and un-compiled source code, to include all versions, maintenance updates and patches (if applicable)
- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes
- Disposition of Contractor purchased Government owned assets, including facilitiesequipment, furniture, phone lines, computer equipment, etc.
- Transfer and documentation of the delivery/return of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable DHA debriefing and personnel out-processing procedures
- Turn-in of all government keys, ID/access cards, and security codes

The contractor will propose activities, schedules, quality control and risk mitigation steps and strategies to include expected outcomes as part of their Transition to integrated Site/Enterprise IT Support Model.

The contractor shall comply with transition-out requirements of the DHA for contractors who have been issued a CAC or who generate "records", as defined by DoD (records manual), including DoD-directed disposition of records, and others displayed on the In/Out (I/O) Processing Portal.

1.7 Administrative specifications

1.7.1 **Place of performance**: The work shall be performed at Government facilities, as indicated in Attachment 7, unless otherwise stated or required by Government. .

1.7.2 **Recognized Federal holidays:** The contractor may be required to perform services on holidays.

New Year's Day
Martin Luther King Jr.'s Birthday
President's Day
Memorial Day
Juneteenth Day
Independence Day
Labor Day
Columbus Day
Veteran's Day
Thanksgiving Day
Christmas Day

1.7.3 **Hours of operation**: The contractor is responsible for conducting business Monday through Friday except federal holidays or when the government facility is closed due to local or national emergencies, administrative closings, or similar government directed facility closings. The contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the government facility is not closed for the above reasons.

Work hours shall continue at most recent order schedule. The contractor may be required to work outside the typical hours of 7:30 a.m. to 4:30 p.m., Monday through Friday excluding federal holidays to satisfy government requirements for a variety of situations, including emergencies or maintenance subject to system availability constraints. It is expected that to the maximum extent practicable, the contractor will offset/credit hours worked outside the normal duty time with less hours during normal duty time for that billing period, the Government expects credit hours to eliminate or minimize request for After Hours support. Periods of absence in excess of 8 workdays in CONUS, or 12 workdays OCONUS cumulative within a single month per FTE, whether for leave or any reason, must be reported and coordinated with the COR. The monthly price will be reduced by the appropriate contract incremental FTE price for each FTE in the billing period that leave exceeds 8 workdays CONUS or 12 workdays OCONUS. Periods of leave 8 workdays or less CONUS / 12 workdays or less OCONUS will not require adjustment of the monthly price.

1.7.4 **Emergency Services**: On occasion, services may be required to support an activation or exercise of contingency plans outside the normal duty hours.

1.8 Contractor travel: Contractor shall be authorized travel expenses consistent with the cost principles and procedures in Federal Acquisition Regulation (FAR) Part 31.2, Travel Costs and the limitations of funds specified in this contract. All travel requires Government

approval/authorization and notification to the Contracting Officer Representative (COR).

Travel shall be approved per the terms and conditions of the task order. All receipts for airfare, rental car, lodging, and all receipts directly being charged for over $75.00 shall be submitted as support/back up documentation with the invoice submittal. NO PAYMENT WILL BE MADE WITHOUT DOCUMENTATION/RECEIPTS. NO PAYMENT WILL BE MADE for travel that is non-conforming to the Federal Travel Regulation (FTR).

Travel shall be approved per the terms and conditions of the task order. All receipts for airfare, rental car, lodging, and all receipts directly being charged for over $75.00 shall be submitted as support/back up documentation with the invoice submittal. NO PAYMENT WILL BE MADE WITHOUT DOCUMENTATION/RECEIPTS. NO PAYMENT WILL BE MADE for travel that is non-conforming to the Federal Travel Regulation (FTR).

All travel shall be scheduled at least two weeks in advance whenever possible to maximize savings to the Government through receiving the best travel rates available. Emergency requirements shall be defined and approved by the COR. All travel shall be in accordance with the FTR and shall be at or below per diem unless approved via CTP. The contractor is required to ensure good stewardship of travel funds and shall seek rates lower than per diem whenever possible.

Contractor shall be authorized travel expenses consistent with the cost principles and procedures in Federal Acquisition Regulation (FAR) Part 31.2, Travel Costs and the limitations of funds specified in this contract. All travel requires Government approval/authorization and notification to the COR. Arrangements for and costs of all travel, transportation, meals, lodging, and incidentals are the responsibility of the Contractor. Travel costs shall be incurred and billed in accordance with the Joint Travel Regulations (JTR). Costs for these expenses will be reviewed, certified and approved by the COR. All travel and transportation shall utilize commercial sources and carriers. The Government will not pay for business class or first-class travel.

Local Travel: The contractor may be required to travel within CONUS to participate in conferences, meetings or other events. Local travel within a 50-mile radius from the individuals' primary place of performance will not be reimbursed (e.g. subsistence, travel time, or other travel related expenses)

Non-Local Travel: The contractor may be required to travel within CONUS to participate in conferences, meetings or other events. Travel greater than a 50-mile radius from the individuals' primary place of performance is considered non-local travel and will be reimbursed, in accordance with Federal Acquisition Regulation (FAR) Part 31 subpart 31.205-46 Travel Costs, only when approved in advance by the Contracting Officer Representative (COR). All travel shall be scheduled at least two weeks in advance whenever possible to maximize savings to the Government through receiving the best travel rates available. The Contractor shall ensure that assigned participants allow sufficient lead-time to obtain valid passports, country clearances, and immunizations to support project activities. All travel outside of the U.S. required under this tasking shall be in accordance with the JTR. Emergency requirements shall be defined and approved by the COR.

Travel must have been preapproved by the COR, and contractor travel must have occurred in order to be invoiced. All travel and transportation shall utilize commercial sources and carriers. The Government shall not pay for business class or first-class travel. The Government will not allow any burden rates applied to travel costs. No burdens or indirect rates may be charged to Travel CLINs. Only direct travel costs that the COR has preapproved, and that the COR finds allowable and allocable may be charged to the contract. No profit nor fee shall be added.

Trip Reports CONUS: When requested, the Contractor shall submit a trip report within 5 working days after completion of travel.

When requested by the Government Task Lead, the contractor shall submit Trip Reports when submitting monthly invoices.

The Trip Report shall include the following information (minimum requirement):

- Personnel traveled
- Dates of travel
- Destination(s)
- Purpose of Trip; contract effort supported and Task Order ID number; Government Agency supported (if applicable), explain the benefits of the travel to the Government.
- Actual Trip Costs/Receipts
- Approval Authority
- Summary of events

1.9 Other Direct Costs (ODC): Actual ODC purchases must have been preapproved by the COR and contractor purchases of COR approved ODC expenses must have occurred in order to be invoiced. All excess funding not used will be deobligated from the ODC CLIN. The Government will not allow any burden or indirect costs may be applied to ODC's. Only direct costs that the COR has preapproved, and that the COR finds allowable and allocable may be charged to the contract. It is the responsibility of the contractor to manage the ODC CLIN amount through the duration of the contract; as no additional funding will be provided. All ODCs shall be fully supported in compliance with all competition requirements of the FAR, specifically Part 31. All ODCs shall be reported as stated in the Procurement of Hardware, Software, Equipment and Materials Section 2.2.3.1, as well as the Monthly Progress Report Section 1.14.6.

Overseas Housing Allowance: The Government will reimburse the Contractor for Overseas Housing Allowance paid to employees assigned to provide on-site support to an OCONUS MTF, not to exceed the rate provided by the JTR. Within one month after task order award or employee assignment to an overseas location whichever is later, the Contractor shall submit, for each employee assigned to an overseas location, written estimates of costs, or actual costs if they are known. Quarterly, thereafter (March, June, September and December), the Contractor shall validate the need and amount of the Overseas Housing Allowance (OHA) by submitting the actual annual expenses of rent and utilities, supported by receipts or other satisfactory evidence, for each employee assigned to an overseas location. (CDRL A009)

ODC's may include Overseas Housing Allowance, OCONUS Cost of Living Allowance,

OCONUS Dependent Education Expense Materials, Relocation Travel Conference Room reservations for offsite meetings, Office supplies/Exhibit Booth supplies, SW subscriptions, training (pre-approved by the Government outside Normal IA Security directives and Requirements) and devices, equipment or peripherals.

All equipment or supplies purchased under the terms of this PWS must adhere to all DOD, regulatory, or other governmental guidelines for security or performance.

1.10 Quality

1.10.1 **Quality Control (QC):** The contractor shall develop and maintain an effective QC program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure nonrecurrence of defective services. The contractor's QC program is the means by which the work complies with stated requirements. The QCP is to be delivered with the contractor's proposal and a comprehensive written QCP shall be submitted to the CO and COR within 5 working days when changes are made thereafter. After acceptance of the QCP the Contractor shall receive the contracting officer's (CO) acceptance in writing of any proposed change to its quality control system. See Part 7,Technical Exhibit 1Quality Control Plan (QCP) (CDRL) A001.

1.10.2 **Quality assurance (QA):** The government will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan provides a systematic method for the Government to evaluate performance and to ensure that the contractor has performed 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).

Quality Control Plan – CDRL A001
The Contractor shall prepare and adhere to a Quality Control Plan (QCP). The QCP shall document how the Contractor will meet and comply with the quality standards established in this statement of work. At a minimum, the QCP must include a self-inspection plan, an internal staffing plan, and an outline of the procedures that the Contractor will use to maintain quality, timeliness, responsiveness, customer satisfaction, and any other requirements set forth in this solicitation.

1.10.3 **Contingency Operations Plan:** CDRL A008 - The Contractor shall develop and submit a Contingency Operations Plan to the Government. The Contingency Operations Plan shall be due ten (10) calendar days after the award of the order, and will be updated yearly. The Contingency Operations Plan shall document Contractor plans and procedures to maintain DHA support during an emergency. The Contingency Operations Plan shall include the following:

- A description of the Contractor's emergency management procedures and policy
- A description of how the Contractor will account for their employees during an emergency
- Planned temporary work locations or alternate facilities
- How the Contractor will communicate with DHA during emergencies

- A list of primary and alternate Contractor points of contact, each with primary and alternate: telephone numbers, e-mail addresses
- Procedures for protecting Government furnished equipment (if any)
- Procedures for safeguarding sensitive and/or classified Government information (if applicable)

1.11 Contractor personnel

1.11.1 **CAC requirements:** For all contractors who will work in Government facilities, the Facilities Security Officer (FSO)/Company's Security point of contact (POC) will provide the Government all the required information per the DHA CAC request process current version 2.1, January 2018, or more recent when updated. See process attached at Part 7 Section 7.1.1 of the PWS. A CAC is the standard identification for eligible DoD contractor personnel.

1.11.1.1 The Contractor shall return all CACs to the COR upon the departure of the Contractor(s).

1.11.2 **Contractor onboarding and training:** The contractor shall complete all requirements, training, and forms as prescribed in the following requirements:

1.11.2.1 "Onboarding Checklist for Contractor Employees" is located at the DHA Onboarding and Offboarding Portal at *https://info.health.mil/cos/admin/hr/IO/SitePages/Home.aspx*

1.11.2.2 The DHA's contractor training instructions embedded at Part 7 Section 7.1.2. *(Government (DHA) requirements development staff must cut/paste onboarding checklist at https://info.health.mil/sites/DOP/OnboardingCtr/Contractor_OnBoarding_Checklist.pdf and embed most up-to-date form in Part 7, Section 7.1.2.)*

1.11.2.3 The contractor shall comply with onboarding requirements of the DHA for contractors needing to be issued CAC identification, including DoD- and DHA-directed training and forms submission, prior to network access, as displayed in the In/Out-Processing Portal at: *https://info.health.mil/cos/admin/hr/IO/SitePages/home.aspx* (note: Public Key Infrastructure (PKI)-restricted, printed versions available).

1.11.2.4 The DHA's new employee handbook at Part 7 Section 7.1.4.

1.11.3 **Physical Security:** 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.

1.11.4 **Key control:** The contractor shall establish and implement methods of making sure all keys/key cards issued to the contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the contractor by the Government shall be duplicated. The contractor shall develop procedures covering key control that shall be included in the QCP. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas.

The contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the CO.

1.11.4.1 In the event keys, other than master keys, are lost or duplicated, the contractor shall, upon direction of the CO, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the contractor.

1.11.4.2 The contractor shall prohibit the use of Government issued keys/key cards by any persons other than the contractor's employees. The contractor shall prohibit the opening of locked areas by contractor employees to permit entrance of persons other than contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the CO.

1.11.5 **Lock combinations**: The contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the contractor's QCP.

1.12 Key personnel (Contractor): The Task Manager and the three (3) contractor Regional Senior Engineers shall be designated as Key Personnel. The Government reserves the right to pre-approve any replacement or substitution of Key Personnel. Contractor personnel must submit necessary information to be issued a clearance prior to reporting for performance. The contractor shall provide a contract manager who shall be responsible for the performance of the work. The name of this person and an alternate who shall act for the contractor when the manager is absent shall be designated in writing to the KO and CO. The contract manager or alternate shall have full authority to act for the contractor on all contract matters relating to daily operation of this contract. The contract manager or alternate shall be available between 7:30 a.m. to 4:30 p.m., Monday thru Friday except Federal holidays. Other Key Personnel are the Senior Network Engineers for CONUS, Europe, and Pacific Regions.

1.12.1 **Senior Network Engineer for CONUS**

1.12.1.1 Responsibilities: The Senior Network Engineer for CONUS region supports the medical mission of the DoD and ensures that the highly complex and technical requirements related to the infrastructure are addressed. The Senior Network Engineer for CONUS is a key personnel, and identifies and resolves larger, more complex LAN/WLAN/WAN network problems and issues, researches network-level problems using network management tools and is responsible for providing high-level installation, configuration, documentation, management and troubleshooting of LAN/WLAN/WAN communication equipment for all DHA networked facilities. Serves as the premier Network Specialist for this contract; subject matter expert for all issues covered under the other jobs discussed within.

Serves as the CONUS, as well as global, point of contact for network issues, configuration management and communications interconnection, addressing, and multi-protocol routing and network management.

Advises and consults with government staff, agencies and other contractor representatives involved with LAN/WLAN/WAN design, network implementation, network deployment, and network management to ensure the LAN/WLAN/WAN adequately supports the MHS mission and provides optimal performance. Interfaces with and leads Network Specialists and internal or external organizations to resolve LAN/WLAN/WAN issues.

The Senior Network Engineer for CONUS region is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Orion SolarWinds, ARMIS, and Ansible. An understanding of Management Information Blocks (MIB) and MRTG to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for the increasing levels of LAN/WLAN/WAN security in maintaining the LAN/WLAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the Senior Network Engineer must be capable of establishing and configuring network firewalls, VPN devices and IDSs.

Provides written recommendations to personnel in the field by making either a change to network level operations or an enhancement to the network (tuning or upgrade), and documenting the change via a ticket, creating a written standard, or updating the written standards already in place by coordinating with the NetMOD Network Standards Team. Studies vendor products to determine which components and configurations best meet the requirements of DoD and MTFs in the Pacific region. Establishes and implements LAN/WLAN/WAN procedures and standards to ensure compliance with DoD and DHA Command objectives and policies. Communicates with key customers on the status of all network support requests.

Beyond network design and implementation, the engineer continuously evaluates and resolves complex technical issues associated with network and routing protocols at all levels of the Open Systems Interconnection (OSI) model through the use of diagnostics and network administration tools. Provides proactive input on policies and issues related to standardization as well as develop and write policies and procedures that identify best practice solutions necessary for operations in support of the LAN/WLAN/WAN. Defines and establishes minimum standards related to LAN/WLAN/WAN access and its impact on overall network operations. Leads/participates on other projects and support as the need arises.

1.12.1.2 QUALIFICATIONS: Compliance with Department of Defense (DoD) Directive DoDD 8140.01 “CYBERSPACE WORKFORCE MANAGEMENT” and DoDI 8140.02 “IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE WORKFORCE REQUIREMENTS” is required. Must have and maintain certification(s) compliant with the Network Operations Specialist “Advanced”, per DoD 8140, “Cyber Workforce Qualification Program Qualification Matrix and Training Repository”.

Ability to carry out functions of all subordinate positions listed in this Labor Category synopsis, should the individual be tasked with traveling to any site covered by this contract.

1.12.1.3 EXPERIENCE: The Senior Network Engineer for the CONUS region must have a mastery of normal networking protocols and technologies, such as TCP/IP, XDM, HTTP, HTTPS, SMTP, SNMP, DNS, DHCP, RSTP, VRRP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and a clear understanding of the 802.1d, 802.1q, 802.1w, 802.3, 802.5, 802.10, 802.11, 802.3u, 803.2, and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate a clear understanding and direct experience with synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, and other communications medium in use by the DoD and DHA. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications are also required.

Possess a mastery level of experience in routed, switched and shared LAN environments that operate such items as current supported versions of Microsoft OS, Windows Active Directory, UNIX and OpenVMS and employ routers, switches, and terminal servers as well as various local and long-haul WAN connectivity.

1.12.1.4 Education: Bachelor's Degree in Computer Sciences, Engineering, technical degree or related discipline, and five years of directly related experience; or successful completion of a certified Technical or Vocational School and 10 years of directly related experience gained through progressively higher levels of complexity.

1.12.1.5 Other Skills: Experience with DoD Health Care Information Systems is required. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems, and Orion SolarWinds. Experience with Zero Trust Architectures and Methodologies is desired; Cisco Certified Network Professional (CCNP) and Certified Information Systems Security Professional (CISSP) are required.

1.12.1.6 Background: A “SECRET” security level designation is required for this position.

1.12.1.7 Verbal & Written Communication Skillls: Must be able to communicate effectively with a broad audience to include Government officials, medical professionals and highly specialized technical personnel, both verbally and in writing.

1.12.2 **Senior Network Engineer for Pacific Region**

1.12.2.1 Responsibilities: The Senior Network Engineer for the Pacific region supports the medical mission of the DoD and ensures that the highly complex and technical requirements related to the infrastructure are addressed. The Senior Network Engineer for Pacific is a key personnel, and identifies and resolves larger, more complex LAN/WLAN/WAN network problems and issues, researches network-level problems using network management tools and is responsible for providing high-level installation, configuration, documentation, management and

troubleshooting of LAN/WLAN/WAN communication equipment for all DHA networked facilities within the Pacific Region.

Serves as the regional point of contact for network issues, configuration management and communications interconnection, addressing, and multi-protocol routing and network management.

Advises and consults with government staff, agencies and other contractor representatives involved with LAN/WLAN/WAN design, network implementation, network deployment, and network management to ensure the LAN/WLAN/WAN adequately supports the MHS mission and provides optimal performance. Interfaces with and leads Network Specialists and internal or external organizations to resolve LAN/WLAN/WAN issues.

The Senior Network Engineer for the Pacific region is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Orion SolarWinds, ARMIS, and Ansible. An understanding of Management Information Blocks (MIB) and MRTG to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for the increasing levels of LAN/WLAN/WAN security in maintaining the LAN/WLAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the Senior Network Engineer must be capable of establishing and configuring network firewalls, VPN devices and IDSs.

Provides written recommendations to personnel in the field by making either a change to network level operations or an enhancement to the network (tuning or upgrade), and documenting the change via a ticket, creating a written standard, or updating the written standards already in place by coordinating with the NetMOD Network Standards Team. Studies vendor products to determine which components and configurations best meet the requirements of DoD and MTFs in the Pacific region. Establishes and implements LAN/WLAN/WAN procedures and standards to ensure compliance with DoD, DHA, and DHA Pacific Regional Command objectives and policies. Communicates with key customers on the status of all network support requests.

Beyond network design and implementation, the engineer continuously evaluates and resolves complex technical issues associated with network and routing protocols at all levels of the Open Systems Interconnection (OSI) model through the use of diagnostics and network administration tools. Provides proactive input on policies and issues related to standardization as well as develop and write policies and procedures that identify best practice solutions necessary for operations in support of the LAN/WLAN/WAN. Defines and establishes minimum standards related to LAN/WLAN/WAN access and its impact on overall network operations. Leads/participates on other projects and support as the need arises.

1.12.2.2 QUALIFICATIONS: Compliance with Department of Defense (DoD) Directive DoDD 8140.01 “CYBERSPACE WORKFORCE MANAGEMENT” and DoDI 8140.02 “IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE WORKFORCE

REQUIREMENTS" is required. Must have and maintain certification(s) compliant with the Network Operations Specialist "Advanced", per DoD 8140, "Cyber Workforce Qualification Program Qualification Matrix and Training Repository".

1.12.2.3 EXPERIENCE: The Senior Network Engineer for the Pacific region must have a mastery of normal networking protocols and technologies, such as TCP/IP, XDM, HTTP, HTTPS, SMTP, SNMP, DNS, DHCP, RSTP, VRRP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and a clear understanding of the 802.1d, 802.1q, 802.1w, 802.3, 802.5, 802.10, 802.11, 802.3u, 803.2, and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate a clear understanding and direct experience with synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, and other communications medium in use by the DoD and DHA. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications are also required.

Possess a mastery level of experience in routed, switched and shared LAN environments that operate such items as current supported versions of Microsoft OS, Windows Active Directory, UNIX and OpenVMS and employ routers, switches, and terminal servers as well as various local and long-haul WAN connectivity.

1.12.2.4 Education: Bachelor's Degree in Computer Sciences, Engineering, technical degree or related discipline, and five years of directly related experience; or successful completion of a certified Technical or Vocational School and 10 years of directly related experience gained through progressively higher levels of complexity.

1.12.2.5 Other Skills: Experience with DoD Health Care Information Systems is required. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems, and Orion SolarWinds. Experience with Zero Trust Architectures and Methodologies is desired; Cisco Certified Network Professional (CCNP) and Certified Information Systems Security Professional (CISSP) are required.

1.12.2.6 Background: A "SECRET" security level designation is required for this position.

1.12.2.7 Verbal & Written Communication Skills: Must be able to communicate effectively with a broad audience to include Government officials, medical professionals and highly specialized technical personnel.

1.12.3 **Senior Network Engineer for EUROPE**

1.12.3.1 Responsibilities: The Senior Network Engineer for Europe supports the medical mission of the DoD and ensures that the highly complex and technical requirements related to the infrastructure are addressed. The Senior Network Engineer for Europe is a key personnel, and identifies and resolves larger, more complex LAN/WLAN/WAN network problems and issues, researches network-level problems using network management tools and is responsible for

providing high-level installation, configuration, documentation, management and troubleshooting of LAN/WLAN/WAN communication equipment for all DHA networked facilities within the Pacific Region.

Serves as the regional point of contact for network issues, configuration management and communications interconnection, addressing, and multi-protocol routing and network management.

Advises and consults with government staff, agencies and other contractor representatives involved with LAN/WLAN/WAN design, network implementation, network deployment, and network management to ensure the LAN/WLAN/WAN adequately supports the MHS mission and provides optimal performance. Interfaces with and leads Network Specialists and internal or external organizations to resolve LAN/WLAN/WAN issues.

The Senior Network Engineer for Europe is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Orion SolarWinds, ARMIS, and Ansible. An understanding of Management Information Blocks (MIB) and MRTG to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for the increasing levels of LAN/WLAN/WAN security in maintaining the LAN/WLAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the Senior Network Engineer must be capable of establishing and configuring network firewalls, VPN devices and IDSs.

Provides written recommendations to personnel in the field by making either a change to network level operations or an enhancement to the network (tuning or upgrade), and documenting the change via a ticket, creating a written standard, or updating the written standards already in place by coordinating with the NetMOD Network Standards Team. Studies vendor products to determine which components and configurations best meet the requirements of DoD and MTFs in the Europe region. Establishes and implements LAN/WLAN/WAN procedures and standards to ensure compliance with DoD, DHA, and DHA European Regional Command objectives and policies. Communicates with key customers on the status of all network support requests.

Establishes and implements LAN/WLAN/WAN procedures and standards to ensure compliance with DoD and European Regional Command objectives and policies. Communicates with key customers on the status of all network support requests.

Beyond network design and implementation, the engineer continuously evaluates and resolves complex technical issues associated with network and routing protocols at all levels of the Open Systems Interconnection (OSI) model through the use of diagnostics and network administration tools. Provides proactive input on policies and issues related to standardization as well as develop and write policies and procedures that identify best practice solutions necessary for operations in support of the LAN/WLAN/WAN. Defines and establishes minimum standards

related to LAN/WLAN/WAN access and its impact on overall network operations. Leads/participates on other projects and support as the need arises.

1.12.3.2 QUALIFICATIONS: Compliance with Department of Defense (DoD) Directive DoDD 8140.01 “CYBERSPACE WORKFORCE MANAGEMENT” and DoDI 8140.02 “IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE WORKFORCE REQUIREMENTS” is required. Must have and maintain certification(s) compliant with the Network Operations Specialist “Advanced”, per DoD 8140, “Cyber Workforce Qualification Program Qualification Matrix and Training Repository”.

Ability to carry out functions of all subordinate positions listed in this Labor Category synopsis, should the individual be tasked with traveling to any site covered by this contract.

1.12.3.3 EXPERIENCE: The Senior Network Engineer for Europe must have a mastery of normal networking protocols and technologies, such as TCP/IP, XDM, HTTP, HTTPS, SMTP, SNMP, DNS, DHCP, RSTP, VRRP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and a clear understanding of the 802.1d, 802.1q, 802.1w, 802.3, 802.5, 802.10, 802.11, 802.3u, 803.2, and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate a clear understanding and direct experience with synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, and other communications medium in use by the DoD and DHA. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications are also required.

Possess a mastery level of experience in routed, switched and shared LAN environments that operate such items as current supported versions of Microsoft OS, Windows Active Directory, UNIX and OpenVMS and employ routers, switches, and terminal servers as well as various local and long-haul WAN connectivity.

1.12.3.4 Education: Bachelor's Degree in Computer Sciences, Engineering, technical degree or related discipline, and five years of directly related experience; or successful completion of a certified Technical or Vocational School and 10 years of directly related experience gained through progressively higher levels of complexity.

1.12.3.5 Other Skills: Experience with DoD Health Care Information Systems is required. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems, and Orion SolarWinds. Experience with Zero Trust Architectures and Methodologies is desired; Cisco Certified Network Professional (CCNP) and Certified Information Systems Security Professional (CISSP) are required.

1.12.3.6 Background: A “SECRET” security level designation is required for this position.

1.12.3.7 Verbal & Written Communication Skills: Must be able to communicate effectively with a broad audience to include Government officials, medical professionals and highly specialized technical personnel, both verbally and in writing.

1.13 Data rights: The Government will retain rights to all data produced in the course of developing, deploying, training, using and supporting DHA or other federal agencies that utilize this order.

1.14 Reporting

1.14.1 **Contractor Manpower Reporting (CMR):** (CDRL A006). At a minimum, on a monthly basis, the contractor shall provide the COR an updated list of personnel in accordance with Part 7, Section 7.3, CRDL A002.

1.14.2 **Non-Disclosure Agreement (NDA):** (CDRL A003) All contractor personnel who will obtain access to proprietary, classified, or confidential information or any information release of which is protected or governed by law or regulation associated with DHA acquisitions shall be required to complete and sign a DHA contractor NDA (DHA Form 49) prior to beginning work on the subject contract. The contractor shall execute an NDA on behalf of the company and shall ensure that all staff assigned to, including all subcontractors and consultants, or other personnel performing on contract/Task order execute an NDA protecting the procurement sensitive information of the Government and the proprietary information of other contractors. The NDA shall be executed not later than first day of employment and to be renewed upon exercising a contract option period. Assignment of staff who has not executed this statement or failure to adhere to this statement shall constitute default on the part of the contractor. The contractor shall maintain originally signed NDAs of individual employees and provide copy to the COR.

1.14.3 **Government's COR:** The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the contractor performs the technical requirements of the contract; perform inspections necessary in connection with contract performance; maintain written and oral communications with the contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor contractor's performance and notifies both the CO and contractor of any deficiencies; coordinate availability of government furnished property; and provide site entry of contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting contract.

1.14.4 **Post award conference/periodic progress meetings:** The contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with FAR Subpart 42.5. The CO, COR, and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the CO will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any,

being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.14.5 **Weekly Vacancy Report – CDRL A004**

The Contractor shall provide a weekly report on the vacancies across all locations. The exact content of this report will be determined after task order award by the COR after collaboration with the Contractor.

1.14.6 **Monthly Progress Report (MPR) - CDRL A005**

The Contractor shall prepare and deliver a Monthly Progress Report, The MPR shall outline the following:

- Expenditures
- Progress (i.e. performance against schedule)
- Status
- Significant events
- Customer Satisfaction – Report customer satisfaction rate every six months showing percentage of completed survey forms that qualitatively demonstrate customer satisfaction with DHA's provision of service
- Trouble Ticket Resolution for Tier 0 (i.e not escalated to the Network Support Center) - Report percentage of calls resolved at the site • Tier 0 Trouble Tickets opened, in progress, resolved and closed during the month
- LAN/WAN issues
- TCP/IP address changes
- Circuits in-use
- Circuits no longer in-use
- Circuits connected
- Circuits disconnected
- Circuit upgrades completed
- Updates to the network physical configuration topology diagrams
- LAN downtime
- WAN downtime
- Remote circuit uptime
- Router configuration changes

The MPR shall also include the following information by facility:

- Firewall/Security Suite configuration changes
- Miscellaneous monthly changes and other significant events
- Schedule of planned activities
- Activities completed to date
- Remaining activities, if applicable (plans vs. achievements)
- Lessons learned
- Risks and mitigation of risks
- Any government action needed
- Monthly ITSM tier 0 (initiated at site) ticket summary
- Document problems encountered and provide the resultant impacts.

- Other information requested by DHA on a recurring or as requested basis.

1.15 Contractor Identification

1.15.1 Contractor personnel performing services in a contractor capacity in a Government facility are required to possess and wear an identification badge that displays his or her name and the name of their company. All contractor personnel shall identify themselves as contractor support personnel in all forms of communication with all entities with whom DHA/Deputy Assistant Director for Acquisition (DAD-A)/Head of the Contracting Activity (HCA) has business dealings. The contractor shall: Answer all telephone calls and have a personalized voice message with an introductory statement that includes the fact that the person is contractor support personnel. Ensure all those with whom the person interacts in any face-to-face dealings while supporting the DAD-A understands that the person is contractor support personnel. Include a title block in all emails that states the fact that the person is contractor support personnel. Ensure all those with whom the person interacts in any face-to-face dealings while supporting DHA/DAD-A/HCA understands that the person is contractor support personnel.

1.15.2 Contractor personnel will be required to attend meetings or otherwise communicate with Government and/or other contract representatives to meet the requirements of this order. Contractor personnel shall make their contractor status known during introductions.

1.15.3 Contractor personnel, while performing in a contractor capacity, are prohibited from using their retired or reserve component military rank or title in any written or verbal communications associated with the contracts in which they provide services.

1.16 Contractor Access to Health Affairs (HA)/DHA Network(s)

1.16.1 FSO/Company's Security POC shall notify the DHA Personnel Security Office after being awarded a contract that requires access to a DoD system (. Contractor personnel requiring access to the HA/DHA networks for performance of their tasks require a background investigation and the security awareness training. The contractor shall be prepared for this process as it could take two (2) or more weeks. The FSO/Security POC shall submit a Standard Form (SF) 85/86 to DHA's Personnel Security Office for a background investigation.

1.16.2 Company's FSO/Security POC must notify the Personnel Security Office when the contractor has submitted the SF-85/86. The FSO/Security POC, or the COR must notify the DHA Personnel Security Office in writing of a contractor's termination from the contract, including the termination date.

1.17 Personnel Security

1.17.1 The contractor shall comply with DoD 8570.01-M, “Information Assurance Workforce Improvement Program, CH4” November 10, 2015 as amended; 8500.01, “Cybersecurity”, dated March 14, 2014; DoD Manual (DoDM) 6025.18, “Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs” dated March 3, 2019, Department of Defense Instruction (DoDI) 6025.18 “HIPAA Privacy Rule Compliance in DoD Health Care Programs”, dated March 13, 2019; and DoDM 5200.02 “Procedures for the DoD Personnel Security Program (PSP),” incorporation change 3,

effective September 24, 2020. Contractor responsibilities for ensuring personnel security include, but are not limited to, meeting the following requirements:

1.17.1.1 Follow the DHA Personnel Security Office guidelines for submittal of security clearances. Contact the DHA Personnel Security Office for guidance on the appropriate background investigation required for personnel on the contract. The DHA Personnel Security Office can be reached at (703) 275-6038.

1.17.1.2 Initiate, maintain, and document personnel security investigations appropriate to the individual's responsibilities and required access to Controlled Unclassified Information (CUI).

1.17.1.3 DHA Personnel Security Office does not deny any access to any automated information system (AIS), network, or Controlled Unclassified Information (CUI). If a contractor receives an unfavorable background investigation, the request for access will be sent back to the FSO for further action. Any unfavorable adjudication will result in DHA Personnel Security Office not signing off on any access request.

PART 2
2.0 DEFINITIONS, ACRONYMS, AND APPLICABLE PUBLICATIONS/INSTRUCTIONS

2.1 Definitions:

2.1.1 Category D: Information Technology (IT) and Telecommunications Services (called D-Services)

2.1.2 Category R: Support (Professional/Administrative/Management) Services (called R-Services)

2.1.3 Contracting Officer (CO): A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

2.1.4 Contracting Officer's Representative (COR): An individual, including a contracting officer's technical representative (COTR), designated and authorized in writing by the CO to perform specific technical or administrative functions. This individual does NOT have authority to change the terms and conditions of the contract.

2.1.5 Nonpersonal services contract: a contract under which the personnel rendering the services are not subject, either by the contract's terms or by the manner of its administration, to the supervision and control usually prevailing in relationships between the Government and its employees.

2.1.6 Quality Assurance Surveillance Plan (QASP): An organized written document specifying the surveillance methodology to be used for surveillance of contractor performance. The Government may either prepare the QASP or require the offerors to submit a proposed quality assurance surveillance plan for the Government's consideration in development of the Government's plan.

2.2 Acronyms:

AIS	Automated Information System
APL	Approved Products List APL
AQL	Acceptable Quality Level
ARRT	Acquisition Requirements Roadmap Tool
ATO	Authority to Operate
B2B	Business-2-Business
CAC	Common Access Card
CAP	Cloud Access Point
CCEVS	Common Criteria Cybersecurity Evaluation and Validation Scheme
CDI	Covered Defense Information
CE	Computer Environment
CDRL	Contract Data Requirement List

CIO	Chief Information Officer
CJCSM	Chairman of the Joint Chiefs of Staff Manual
CMMC	Cybersecurity Maturity Model Certification
CMR	Contractor Manpower Reporting
CNSSI	Committee on National Security Systems Instruction
CO	Contracting Officer(s)
CONUS	Continental United States (excludes Alaska and Hawaii)
COR	Contracting Officer Representative
COTR	Contracting Officer's Technical Representative
CSP	Cloud Service Provider
CSSP	Cyber Security Service Provider
CUI	Controlled Unclassified Information
DAD-A	Deputy Assistant Director for Acquisition
DC3	DoD Cyber Crime Center
DD Form 254	Department of Defense Contract Security Requirement List (if applicable)
DB	Design-Build
DBB	Design-Bid-Build
DFARS	Defense Federal Acquisition Regulation Supplement
DHA	Defense Health Agency
DISA	Defense Information System Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
DSAs	Data Sharing Agreements
DSAA	Data Sharing Agreement Application
DMZ	Demilitarized Zone
DoDM	Department of Defense Manual
DPCLO	DHA Privacy and Civil Liberties Office
DUA	Data Use Agreement
eMSM	Enhanced Multi-Service Markets
EULA	End User License Agreement
EVM	Earned Value Management
FAR	Federal Acquisition Regulation
FCI	Federal contract information
FE	Facilities Enterprise
FedRAMP	Federal Risk Authorization and Management Program
FISMA	Federal Information Security Modernization Act
FRCS	Facility Related Control Systems
FSO	Facilities Security Officer
HA	Health Affairs
HIPAA	Health Insurance Portability and Accountability Act
HCA	Head of the Contracting Activity
HIT	Health Information Technology
IGCE	Independent Government Cost Estimate
IA	Information Assurance
IO	Initial Outfitting

I/O	In/Out Processing Portal
IPv	Internet Protocol Version
IS	Information System
ISP	Internet Service Provider
IT	Information Technology
ISCM	Information Security Continuous Monitoring
IV&V	Independent Verification & Validation
JTR	Joint Travel Regulations
MedCOI	Medical Community of Interest
MHS	Military Health System
MIL-STD	Military Standard
MTFs	Military Treatment Facilities
NCR	National Capitol Region
NDA	Non-Disclosure Agreement
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
OCONUS	Outside Continental United States (includes Alaska and Hawaii)
ODC	Other Direct Costs
OPM	Office of Personal Management
OSD	Office of the Secretary of Defense
P-ATO	Personal Authorization to Operate
P&R	Personnel and Readiness
PGI	Procedures, Guidance and Information
PDT	Project Delivery Team
PHI	Protected Health Information
PII	Personally Identifiable Information
PIT	Platform Information Technology
PK	Public Key
PKI	Public Key Infrastructure
POA&M	Plan of Action and Milestones
POC	Point of Contact
PMO	Program Management Office
PoP	Period of Performance
PP	Personal Property
PPSM	Ports, Protocols, and Services Management
PRS	Performance Requirements Summary
PSP	Personnel Security Program
PWS	Performance Work Statement
QA	Quality Assurance
QAP	Quality Assurance Program
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
RFP	Request for Proposal
RFQ	Request for Quotation
RMF	Risk Management Framework

SP	Special Publication
SPRS	Supplier Performance Risk System
SRM	Sustainment, Restoration and Modernization
SRG	Security Requirements Guides
STIG	Security Technical Implementation Guides
TM	Task Manager
TOS	Terms of Service
US	United States
UFC	Unified Facilities Criteria
VPN	Virtual Private Network
XML	Extensible Markup Language

2.3 Applicable Publications, DHA Administrative Instructions (AI), etc.

The Contractor shall abide by all current and applicable regulations, publications, manuals, and local policies and procedures, including the following DoD Regulations:

- DoD Instruction Number 8510.01, Risk Management Framework for DoD Information Technology (IT),
- DoD Directive, Defense Health Agency (DHA) DoDD 5136.13
- DoD Instruction 8410.02, NetOps for the Global Information Grid (GIG)
- DoDI 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs
- DoDI 8320.02, Sharing Data, Information, and Technology (IT) Services in the Department of Defense
- DoD Instruction 6490.03, Deployment Health
- DoD Instruction 5400.16, DoD Privacy Impact Assessment (PIA) Guidance
- Joint Publication 3-12 (R) Cyberspace Operations
- DoDI 8500.01, Cybersecurity
- DoD Directive 8000.01, Management of the Department of Defense Information Enterprise
- DoD Directive 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)
- DoD Instruction 6025.19, Individual Medical Readiness (IMR)
- DoD 6025.18-R, DoD Health Information Privacy Regulation
- DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems & Networks
- DoD Instruction 8410.03, Network Management (NM)
- Military Health System OCIO Policy #11
- DoD Instruction 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies
- DoD Instruction 6025.22, Assistive Technology (AT) for Wounded, Ill, and Injured Service Members
- Public Law 104-191, “Health Insurance Portability and Accountability Act of 1996”
- DoD Instruction 6025.19, Individual Medical Readiness (IMR)
- DoD Instruction 8551.01, Ports, Protocols, and Services Management (PPSM)
- DoD 8570.01-M, Information Assurance Workforce Improvement Program

- DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
- Institute of Electrical & Electronics Engineers (IEEE) 802 - Standards for Local and Metropolitan Area Networks: Overview and Architecture.
- Telecommunications Industry Association/Electronic Industries Alliance Standard TIA/EIA-606-A - Administration Standard for the Telecommunications Infrastructure of Commercial Buildings.
- J-STD-607-A - Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications (ANSI/J-STD--607-A - 2002)
- TIA/EIA - 568-B.1 – Commercial Building Telecommunications Cabling Standard – Part 1: General Requirements (ANSI/TIA/EIA-568-B.1-2001)
- TIA/EIA - 568-B.2 – Commercial Building Telecommunications Cabling Standard – Part 2: Balanced Twisted Pair Cabling Components (ANSI/TIA/EIA-568-B.2-2001)
- TIA/EIA – 568-B.3 – Optical Fiber Cabling Components Standard (ANSI/TIA/EIA-568-B.3-2000)
- DoD Regulation 5200.2-R, “DoD Personnel Security Program,"
- DoD Regulation 5000.2-R, "Mandatory procedures for Major Defense Acquisition Programs (MDAP) and Major Automated Information System Acquisition Programs (MAISAPs)," Department of Defense Joint Technical Architecture,
- MHS Automated Information System (AIS) Security Policy Manual,
- MHS Architectural Framework,
- Building Industry Consulting Services International (BICSI), Information Transport Systems Installation Manual (ITSIM),
- Software Engineering Institute Capability Maturity Modeling (SEI CMM), Level 2 procedures and processes
- DoDM 8140.03 “Cyberspace Workforce Qualification and Management Program”
- Army in Europe Regulation 715-9, “Contractor Personnel in Germany – Technical Expert, Troop Care & Analytical Support”

2.4 **Geographic Area Specific**

2.4.1 CONUS: Follow local MTF guidance and policies.

2.4.2 OCONUS: Contractor is responsible for following and understanding all host country specific work requirements and agreements.

PART 3
3.0 GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

The Requiring Activity Authority has assessed the need for Government Furnished Property, Equipment, and Services and determined:

3.1 Services: The Government:

☐ Will **NOT** provide Government Furnished Services in support of this contract/task order. As a result, this paragraph is Not Applicable.

☒ **WILL** provide Government Furnished Services required in support of this contract/task orders. These Services are described below:

Provide Maintenance Contracts
Modernization of equipment, systems, or supplies
Network Monitoring and/or Management Applications
Relevant network security applications, systems, hardware, and integrations

3.2 Facilities: The Government:

☐ Will **NOT** provide Facilities in support of this contract/task order. As a result, this paragraph is Not Applicable.

☒ **WILL** provide Facilities in support of this contract/task orders. The Government provided Facilities are described below:

Office space in the MTFs or Facilities identified in Attachment 7 or attached site locations document

3.3 Utilities: The Government:

☐ Will **NOT** provide Utilities in support of this contract/task order. As a result, this paragraph is Not Applicable.

☒ **WILL** provide Utilities in support of this contract/task orders. The Government provided Utilities are described below:

All utilities in the facility will be available for the contractor's use in performance of tasks outlined in this PWS.

3.4 Equipment: The Government:

☐ Will **NOT** provide Equipment in support of this contract/task order. As a result, this paragraph is Not Applicable.

☒ **WILL** provide Equipment in support of this contract/task orders. The Government provided Equipment is described below:

The Government will provide telephones, facsimile machines, copiers and computer equipment to include laptops for use in performance under this contract/task order. This equipment is authorized for transaction of official Government business only and shall not be used for personal business. Personal long distance calls are not authorized and the cost of all personal long distance calls made by contractor or subcontractor employees may be deducted from the contractor/s invoice payments. Telephones, facsimile machines and computer equipment to include laptops are subject to communications security monitoring at all times. Contractor and subcontract employees may be issued keys signed for at scheduled and unscheduled key control inspections. The contractor shall be required to reimburse the Government for lost keys, or lockset (if lockset is required to be replaced) as a result of lost keys. The cost of replacement of keys/locksets may be deducted from payments to the contractor. Items issued will remain the property of the Government and the contractor will maintain proper accountability of issued equipment. Equipment shall not be removed from the facilities shown in paragraph 3.2 above, unless otherwise specified in the PWS. They are to be used, turned in and/or disposed of as directed by the COR or CO."

3.4.1 **Procurement Integrated Enterprise (PIEE), GFP Module Application** The contractor shall be responsible for obtaining and maintaining access, training and successful operation of the PIEE/GFP Module application for the entirety of the contract/task order PoP. The PIEE GFP Module application is located at the following website: *https://wawf.eb.mil/piee-landing/*. Access to PIEE/GFP Module application training materials and in-depth information applicable to the contractor's responsibilities regarding GFP can be found at the following website: *https://dodprocurementtoolbox.com/*.

Contracting Office Responsibilities:
The Contracting Office shall ensure close coordination and validation of the GFP items with the COR and DHA Accountable Property Officer prior to uploading the GFP Attachment into the PIEE/GFP Module. At the time GFP is anticipated and identified, the Government will upload the GFP Attachment into the PIEE/GFP Module. It is the Contracting Office's responsibility to prepare, upload and maintain the GFP Attachment in the PIEE/GFP Module in accordance with the GFP Attachment instructions provided at the DoD Procurement Toolbox. The CO and COR shall manage and keep an inventory of any GFP associated with contract/task orders awarded through DHA, in accordance with applicable FAR Part 45, DoD FAR Supplement (DFARS) 245 with respective clauses, DHA AI 095 and PD 45-01 following the change in disposition of items listed on that PIEE/GFP Module Attachment.

The contracting office will also review, acknowledge, reject and/or approve shipment orders provided by the contractor as appropriate. Functional roles can be determined within the Contracting Office, and requested within the PIEE/GFP Module system.

Contractor Responsibilities:
A key contractor responsibility is to work with the CO and COR to ensure the PIEE/GFP Module data, to include the PIEE/GFP Attachment, provides a timely, complete and accurate accounting of the GFP applicable to the contract/task order. Contractors are required to report the receipt of any GFP shipped to them, regardless of whether it is listed on the GFP Attachment for their contract. Similarly, contractors are required to utilize the GFP Module application in conjunction with the shipment of GFP to the Government, or in reporting Property Loss of GFP issued (such as destruction or loss). Discrepancies or disputes regarding property shipped to or shipped from the contractor must be reported via the GFP Module application, with the CO having authority over final designation of status.

3.5 Materials: The Government:

☒ Will **NOT** provide Materials in support of this contract/task order. As a result, this paragraph is Not Applicable.

☐ **IS** providing Materials in support of this contract/task orders. The Government-provided Materials are described below:

PART 4
4.0 CONTRACTOR FURNISHED ITEMS AND SERVICES

4.1 Services: The Contractor:

☒ Will **NOT** provide Contractor Furnished Services in support of this contract/task order. As a result, this paragraph is Not Applicable.

☐ **WILL** provide Contractor Furnished Services required in support of this contract/task orders. These Services are described below:

_____

_____

4.2 General: The contractor shall furnish all supplies, equipment, facilities and services required to perform work listed under Section 5 of this PWS. Provide required initial and proficiency training for its personnel to maintain pace with technological advances. This training shall be at no additional cost to the government. Contractor shall ensure appropriate employees maintain the required certifications for their specialty.

4.3 Secret Facility Clearance: The contractor shall possess and maintain a SECRET facility clearance from the Defense Security Service. The contractor's employees, performing work in support of this contract shall have been granted a SECRET security clearance from the Defense Industrial Security Clearance Office.

4.4 Materials: N/A

4.5 Equipment: N/A

4.6 Facilities: The contractor when authorized to Remote Work, telework, or work from a non-government facility, the Contractor will ensure their employees have the workspace, telephone, and internet access, sufficient privacy to prevent inadvertent access to HIPAA information or Controlled Unclassified Information, observe all security and OPSEC requirements, and other capabilities necessary to perform their assigned tasks. The Contractor shall be responsible for all communications costs for data access to connect to government networks. Contractor employees shall utilize the Virtual Private Network (VPN), use their Common Access Card (CAC) when performing telework, and stay connected with teammates and government personnel through the use of the DoD-approved chatting tool, such as MS Teams. At a minimum, all contractor employees shall be required to update their CACs and log into their accounts at nearest capable Government installation annually.

PART 5
5.0 SPECIFIC TASKS

5.1 Program Management

The Contractor shall provide sufficient management to ensure that this task is performed efficiently, accurately, on time, and in compliance with the requirements of this document. Specifically, the Contractor shall designate a single manager to oversee this task and supervise staff assigned to this task. (CDRL A007)

5.1.1 **Operations during Emergency Situations**

Individual contingency operation plans shall be activated immediately after determining that an emergency has occurred, shall be operational within twelve (12) hours of activation, and shall be sustainable until the emergency situation is resolved and normal conditions are restored or the task order is terminated, whichever comes first. In case of a life threatening emergency, the COR shall immediately make contact with the Contractor Task Manager to ascertain the status of any Contractor personnel who were located in Government controlled space affected by the emergency. When any disruption of normal, daily operations occur, the Contractor Task Manager shall promptly open an effective means of communication and verify:

- Key points of contact (Government and Contractor)
- Temporary work locations (alternate office spaces, telework, virtual offices, etc.)
- Means of communication available under the circumstances (e.g. email, webmail, telephone, FAX, courier, etc.)
- Essential work products expected to continue production by priority

The Contractor Task Manager, in coordination with the COR, must make use of the resources and tools available to continue DHA contracted functions to the maximum extent possible under emergency circumstances. The Contractor must obtain approval from the COR and Contracting Officer prior to incurring costs over and above those allowed for under the terms of this task order. Regardless of task order type, and of work location, Contractors performing work in support of authorized tasks within the scope of their task order shall charge those hours accurately in accordance with the terms of this task order.

5.1.2 **Contractor Personnel Performance/Replacement**

The contractor Task Manager and the three (3) Regional Senior Engineers shall be designated as Key Personnel. The Government reserves the right to pre-approve any replacement or substitution of Key Personnel.

Contractor personnel must submit necessary information to be issued a clearance prior to reporting for performance.

5.1.3 **Contractor Training, Position Responsibilities and Qualifications**

The Contractor is required to provide personnel trained in systems, equipment, and software identified in attachment 7 ‘Labor Category Responsibilities and Required Qualifications’ (Updated 09.21.2020). This attachment outlines the position responsibilities and qualifications,

including any necessary experience, education, and/or other skills required according to location assignment.

Government training: The Contractor shall ensure that all Contractor employees attend or successfully complete all mandatory Government training. The training typically encompasses matters of security and safety, and is provided during billable time at no cost to the Contractor. Any additional training needed for newly deployed systems will be billable, at no cost to the Contractor.

When operating Government owned or leased equipment, the Contractor shall ensure proper security clearance, (ADP sensitivity I, II, III) full familiarity with operation processes and procedures, and full compliance with site specific regulations, processes and procedures. When performing system operations, the Contractor shall ensure that staff sign and adhere to a Non-disclosure Statement (Appendix C) and protect ALL patient and system information.

5.1.3.1 **Training Workshop**

The Government may choose to hold a training workshop on an annual or semi-annual basis, as needed, with the Contractor employees attending such mandatory workshop. The Contractor shall participate fully with the Government in the planning, organization, and all aspects of such workshops. The training will be provided at a date, time and location decided by the Government during billable time at no cost to the Contractor.

5.2 **Network Support**

The Contractor shall provide remote and/or on-site network (i.e. local, wireless, and wide area network) sustainment and deployment support services to the Defense Health Agency (DHA) Medical Treatment Facilities (MTF) and any other DHA Activity, which includes hospitals, clinics, and other remote elements throughout CONUS and OCONUS locations, as described in Section 7 Attachment 7, titled “List of Sites and Associated Support Details”. The Contractor shall support the overall network infrastructure at an MTF and respond to, detect, report, record, diagnose and resolve the occurrence of network faults as well as measure network performance and connectivity on an ongoing basis. The Contractor shall serve as an on-site resource for site coordination, troubleshooting, problem resolution, local inventory interfaces with MTF staff, and shall provide customer service and guidance to the various site staff within the MTFs. The Contractor may be required to provide support to the MTF in the following areas:

- Install, relocate, configure, modify and test routers, switches, wireless access points and associated controllers, and terminal servers.
- Create, maintain and manage Virtual Local Area Networks (VLANs) in accordance with the DHA Standards and Zone Architecture Requirements.
- Install, test, terminate and maintain cable. (Such installation will provide no warranty of installed cable or drops. All material and equipment required will be provided by the Government).
- Troubleshoot wiring problems.
- Certify wiring drops.
- Troubleshoot serial communication lines.
- Operate and maintain compliance with DHA Network Management Systems (NMS) standards, and ensure that 100% of the network infrastructure is communicating with and

reporting in/to the DHA NMS; ensure compliance with device monitoring and configuration backup standards, processes, and procedures.

- Conduct all activities required to support the Site and Enterprise ATO Package(s), such as self-assessments, implementation of security configurations within the timeline required by the severity of the IAVA/CVE or as directed by DHA, device security scans, maintenance of HW/SW Inventory List, etc, for all network infrastructure devices within the purvue of the Site or as directed by DHA.
- Manage network operating systems (NOS) / Firmware and configurations of said network infrastructure devices in compliance with DHA Standards supporting any and all IAVAs/CVEs and STIGs on monthly or on an as needed basis if required completion or compliance basis is sooner.
- Support diagnostics and configuration connectivity of MHS site/service specific servers, such as MHS GENESIS, Defense Medical Logistics Standard Support (DMLSS), Defense Blood Standard System (DBSS), Expense Assignment System (EAS) IV, as well as various office automation and electronic mail systems, suites, and clinical software add-ons, etc.
- Maintain MHS site telecommunications systems if applicable.
- Assist with the establishment and implementation of network policies, procedures and standards to include network security.
- Support the MTF management staff with briefings and updates on network issues.
- Complete DHA furnished Sparing & Maintenance hardware inventories by ensuring all network infrastructure devices are monitored by and reporting to the DHA NMS on atleast a monthly basis, and validate completion via a signed acknowledgment reviewable by the COR/TM.
- Manage and/or Monitor security firewalls/Virtual Private Network (VPN) devices.
- Collect Performance Measurement information and report/respond/remediate any anomalies.
- Assist with DHA Infrastructure Modernization deployments and technical hardware refresh initiatives. Comply with required HW install in the timeframe requested by the Modernization Team, ensuring each piece of equipment is installed, DRMO'd, or sent back to the Modernization Team in the required timeframe, and finally documented within the DHA Ticketing System.
- Participate in long-range MHS infrastructure planning and technical architecture
- Develop, plan and maintain documentation necessary for operations in support of LAN/WLAN to WAN connectivity.
- Define and recommend minimum standards, as applies to network operations, access to the Internet and its impact on overall network resourcing and operations.
- Oversee the integration of network hardware and software platforms for LAN/WLAN connected systems and medical AISs at MTFs, clinics, etc. as directed by the COR.
- Coordinate telecommunications actions with all applicable agencies and organizations as required.
- Address user concerns with the LAN/WLAN/WAN service provider and alert users to routine maintenance impacting circuits.
- Provide network related advice to DoD medical information systems personnel.
- Share information with the contractor's senior engineering staff such as lessons learned and issues requiring higher level technical or management involvement for resolution

5.2.1 **Network Development**
Additionally, the Contractor shall perform infrastructure analysis, integration and support of new technologies and products and communicate with external agencies for site-related activities and implementation actions and provide Technical Reports, Evaluations and Recommendations to include recommendations on technical solutions for regional upgrades, or network changes, such as:

- Evaluate and recommend new and evolving networking technologies.
- Evaluate vendor products.
- Assess data, voice, and video network requirements.
- Propose implementation strategies.
- Propose enhancements or design changes to improve the efficiency of the networks.

5.2.2 **Network Management**

5.2.2.1 The Contractor shall complete DHA furnished Sparing & Maintenance hardware inventories by ensuring all network infrastructure devices are monitored by and reporting to the DHA NMS on atleast a monthly basis, to include adding and removing any equipment provided by and/or refreshed by the DHA Network Modernization Team. This reporting is required to provide a more accurate and more efficient reporting and tracking mechanism of network infrastructure for the DHA Asset Management Team, supporting their activities of providing HW/SW Sustainment through contracts with the applicable Vendors. Completion will be validated and tracked through a signed letter of completion provided by the NE&S as part of the monthly deliverables, spot reviewed by TM and/or COR, with Semi-Annual review by the Asset Management Team. Any changes to the inventory must be annotated in a ITSM Ticket to the AMSR Support Team. Each monthly validation is required to have atleast a 98.5% accuracy rate, and no more than two non-compliant reports per Period-of-Performance (PoP) will be allowed. (CDRL A010)

5.2.2.2 The Contractor shall conduct/attend any walk-through and/or meeting where contractor maintained systems are discussed. The Contractor shall participate in Integrated Product Teams (IPT) as required by the Government.

5.2.2.3 System Support
In the process of providing network support, the Contractor shall be required to interface with MHS systems in troubleshooting network issues and in deliniating between system and network problems. This competency requires a basic knowledge of MHS system infrastructure and application systems, and applicable hardware and software configuration, operation and support skills. The Contractor shall apply any necessary software maintenance processes at, or equivalent to, the SEI CMM Level II, or higher.

5.2.2,3. System Support (Sembach, Germany) – General systems administration support is required for specific Government systems. See description of required support in Attachment E “Systems and Network Specialist (Sembach, Germany).

5.2.3 **Basic Services**

5.2.3.1 As appropriate for skillset utilizing appropriate Standard Operating Procedures (SOPs) and other supporting documentation. Create a written standard, updating the written standards already in place, or other technical and procedural documentation, such as SOPs, checklists, guides, etc. for issues where no guidance exists and to maximize process efficiencies by coordinating with the NetMOD Network Standards Team, ensuring that official standards are maintained and distributed at the enteprise level.

In coordination with and approved by the NetMOD Branch Leadership, create, develop, implement, update, enforce, maintain, and monitor/surveil a Change Enablement Framework, such as an enterprise level change management and change control process for all network infrastructure scoped within this requirement. Utilize this process to test, validate, submit, and secure approval to implement and deploy changes within the production environment, as required by policy and in support of the requirements set by the ATO process for all systems and accreditation boundaries.

Coordinate and follow DHA processes, standards, policies, and procedures for network management.

Manage Information Technology Service Management (ITSM) Incident Management ticket queues. Resolve customer issues, responding to specialized and/or high impact issues on a priority basis and document efforts in the IT system. Perform monthly trend analysis and run ticket queries as necessary to ensure Change Request assessments are completed within 24 hours prior to the scheduled change, or no later than 24 hours after an unscheduled change. Ensure that, using the DHAs Ticketing system, all official tickets, tasks, and workload (including tracking of time per ticket/task) are accurately and properly documented, and resolve any difficiencies within the same reporting period.

Communicate effectively both orally and written with customers, stakeholders, and technical specialists. As required, work directly with customers to resolve issues. Effectively lead detailed technical discussions and develop and present required briefing materials to ensure the customer’s needs are met in accordance with DoD, military Service branches, and DHA requirements. Participate in technical working groups strategizing for future requirements and propose enhancements based on business needs.

5.3 Labor Category Responsibilities and Required Qualifications

JOB TITLE: Referral Network Engineer:

RESPONSIBILITIES: The Referral Network Engineer ensures that the LAN/WAN is capable of providing required services by supporting the network infrastructure through the use of troubleshooting and problem resolution in a production environment. Provides daily operational and sustainment support for all DHA deployed LAN/WLAN/WAN networks within all DHA Activities. Plans, installs and supports hardware and software upgrades, oversees and/or implements all changes to the enterprise in accordance with approved LAN/WLAN/WAN Network Standards.

The Referral Network Engineer is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Orion SolarWinds, ARMIS, and Ansible. An understanding of Management Information Blocks (MIB) and MRTG type tools used to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for the increasing levels of LAN/WLAN/WAN security in maintaining the LAN/WLAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the Referral Network Engineer must be capable of establishing and configuring network firewalls, VPN devices and IDSs.

Uses diagnostic utilities to identify and isolate problems encountered on different mediums and network protocols, gather latency statistics and find specific network bottlenecks, evaluate problems and implement fix actions through device reconfiguration or replacement depending on the circumstances.

QUALIFICATIONS: Compliance with Department of Defense (DoD) Directive DoDD 8140.01 “CYBERSPACE WORKFORCE MANAGEMENT” and DoDI 8140.02 “IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE WORKFORCE REQUIREMENTS” is required. Must have and maintain certification(s) compliant with the Network Operations Specialist “Intermediate”, per DoD 8140, “Cyber Workforce Qualification Program Qualification Matrix and Training Repository”.

EXPERIENCE: The Referral Network Specialist must have a clear understanding and proficient in the normal networking protocols and technologies, such as TCP/IP, XDM, HTTP, HTTPS, SMTP, SNMP, DNS, DHCP, RSTP, VRRP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and a clear understanding of the 802.1d, 802.1q, 802.1w, 802.3, 802.5, 802.10, 802.11, 802.3u, 803.2, and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate a clear understanding and direct experience with synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, and other communications medium in use by the DoD and DHA. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications are also required.

Possess experience in routed, switched and shared LAN environments that operate such items as current supported versions of Microsoft OS, Windows Active Directory, UNIX and OpenVMS and employ routers, switches, and terminal servers as well as various local and long-haul WAN connectivity.

EDUCATION: Bachelor’s degree in a technical discipline such as Computer Sciences and five (5) years related experience; or successful completion of a certified technical/vocational school and eight (8) years related experience.

OTHER SKILLS: Experience with DoD Health Care Information Systems is highly recommended. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Expertise in Windows networks, Cisco Systems, and Orion SolarWinds. Experience with Zero Trust Architectures and Methodologies is desired; Has one or more of the following certifications aligned with the enterprise deployed network architectures: Security+ and Cisco Certified Network Associate (CCNA) or equivalent (i.e., BCNE for Brocade, etc.).

BACKGROUND: An Automated Data Processing (ADP) sensitivity level determination is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must be able to communicate effectively with a broad audience to include Government officials, medical professionals and highly specialized technical personnel, both verbally and in writing.

JOB TITLE: Network Engineer Associate:

RESPONSIBILITIES: The Network Engineer Associate ensures that the LAN/WAN is capable of providing required services by supporting the network infrastructure through the use of troubleshooting and problem resolution in a production environment. Provides daily operational and sustainment support for all DHA deployed LAN/WLAN/WAN networks within all DHA Activities under their pervue. Coodinates with Network Specialists to plan, install and support hardware and software upgrades. Recieves direction from either the Regional Senior Network Engineer and/or the Referral Network Engineer and oversees or implements all changes to the network in accordance with approved LAN/WLAN/WAN Network Standards.

The Network Engineer Associate ensures that the LAN/WAN is capable of providing required services by supporting the network infrastructure through the use of troubleshooting and problem resolution in a production environment. Provides daily operational and sustainment support for all DHA deployed LAN/WLAN/WAN networks within all DHA Activities under their pervue. Coodinates with Network Specialists to plan, install and support hardware and software upgrades. Recieves direction from either the Regional Senior Network Engineer and or the Referral Network Engineer and oversees or implements all changes to the network in accordance with approved LAN/WLAN/WAN Network Standards.

Responsible for the increasing levels of LAN/WLAN/WAN security in maintaining the LAN/WLAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the Network Engineer Associate must be capable of confering with and taking direction from both the Referral Network Engineer and/or the Regional Senior Engineer to establish and configure network firewalls, VPN devices and IDSs.

Uses diagnostic utilities to identify and isolate problems encountered on different mediums and network protocols, gather latency statistics and find specific network bottlenecks, evaluate problems and implement fix actions through device reconfiguration or replacement depending on the circumstances.

QUALIFICATIONS: Compliance with Department of Defense (DoD) Directive DoDD 8140.01 "CYBERSPACE WORKFORCE MANAGEMENT" and DoDI 8140.02 "IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE WORKFORCE REQUIREMENTS" is required. Must have and maintain certification(s) compliant with the Network Operations Specialist "Intermediate", per DoD 8140, "Cyber Workforce Qualification Program Qualification Matrix and Training Repository".

EXPERIENCE: The Network Engineer Associate must have a clear understanding and proficient in the normal networking protocols and technologies, such as TCP/IP, XDM, HTTP, HTTPS, SMTP, SNMP, DNS, DHCP, RSTP, VRRP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and a clear understanding of the 802.1d, 802.1q, 802.1w, 802.3, 802.5, 802.10, 802.11, 802.3u, 803.2, and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate a clear understanding and direct experience with synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, and other communications medium in use by the DoD and DHA. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications are also required.

Possess experience in routed, switched and shared LAN environments that operate such items as current supported versions of Microsoft OS, Windows Active Directory, UNIX and OpenVMS and employ routers, switches, and terminal servers as well as various local and long-haul WAN connectivity.

EDUCATION: Bachelor's degree in a technical discipline such as Computer Sciences and three (3) years related experience; or successful completion of a certified technical/vocational school and five (5) years related experience.

OTHER SKILLS: Experience with DoD Health Care Information Systems is highly recommended. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Highly proficient in Windows networks, Cisco Systems, and Orion SolarWinds. Experience with Zero Trust Architectures and Methodologies is desired; Has one or more of the following certifications aligned with the enterprise deployed network architectures: Security+ and Cisco Certified Network Associate (CCNA) or equivalent (i.e., BCNE for Brocade, etc.).

BACKGROUND: An Automated Data Processing (ADP) sensitivity level determination is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must have strong oral and written communications skills to effectively present information to a broad audience of Government officials, medical professionals, and highly specialized technical personnel.

JOB TITLE: Network Specialist

RESPONSIBILITIES: The Network Specialist ensures that the LAN/WAN is capable of providing required services by supporting the network infrastructure through the use of troubleshooting and problem resolution in a production environment. Provides daily operational and sustainment support for all DHA deployed LAN/WLAN/WAN networks within the DHA Activities under the Network Specialists prevue. Coordinates with Network Engineer Associate or Referral Network Engineer to plan, install and support hardware and software upgrades. Receives direction from either the Referral Network Engineer and/or the Network Engineer Associate and implements all changes to the network in accordance with approved LAN/WLAN/WAN Network Standards.

The Network Specialist is required to resolve technical issues associated with network and routing protocols at all levels of the OSI model through the use of diagnostics and network administration tools such as Orion SolarWinds, ARMIS, and Ansible. An understanding of Management Information Blocks (MIB) and MRTG type tools used to measure, plan and execute methodologies to ensure high performance levels and minimum downtime.

Responsible for the increasing levels of LAN/WLAN/WAN security in maintaining the LAN/WLAN – WAN barrier systems responsible for preventing unauthorized access to MTF systems. In order to meet these requirements, the Network Specialist must be capable of confering with and taking direction from both the Referral Network Engineer and/or the Network Engineer Associate to establish and configure network firewalls, VPN devices and IDSs.

Uses diagnostic utilities to identify and isolate problems encountered on different mediums and network protocols, gather latency statistics and find specific network bottlenecks, evaluate problems and implement fix actions through device reconfiguration or replacement depending on the circumstances.

QUALIFICATIONS: Compliance with Department of Defense (DoD) Directive DoDD 8140.01 “CYBERSPACE WORKFORCE MANAGEMENT” and DoDI 8140.02 “IDENTIFICATION, TRACKING, AND REPORTING OF CYBERSPACE WORKFORCE REQUIREMENTS” is required. Must have and maintain certification(s) compliant with the Network Operations Specialist “Intermediate”, per DoD 8140, “Cyber Workforce Qualification Program Qualification Matrix and Training Repository”.

EXPERIENCE: The Network Specialist must have a clear understanding and proficient in the normal networking protocols and technologies, such as TCP/IP, XDM, HTTP, HTTPS, SMTP, SNMP, DNS, DHCP, RSTP, VRRP, Berkeley Internet Name Domain (BIND), EIGRP, BGP, OSPF, Point to Point Protocol (PPP), High-Level Data Link Control (HDLC), V.35, RS-449 and a clear understanding of the 802.1d, 802.1q, 802.1w, 802.3, 802.5, 802.10, 802.11, 802.3u, 803.2, and 802.3z communications and Internet standards is required. Additionally, the candidate must demonstrate a clear understanding and direct experience with synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, and other communications medium in use by the DoD and DHA. Experience with various Optical Time Domain Reflectometer (OTDR), cable testers, network sniffers and EIA/TIA cable standards and specifications are also required.

Possess experience in routed, switched and shared LAN environments that operate such items as current supported versions of Microsoft OS, Windows Active Directory, UNIX and OpenVMS and employ routers, switches, and terminal servers as well as various local and long-haul WAN connectivity.

EDUCATION: Bachelor's degree in a technical discipline such as Computer Sciences and two (2) years related experience; or successful completion of a certified technical/vocational school and three (3) years related experience.

OTHER SKILLS: Experience with DoD Health Care Information Systems is highly recommended. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Proficient in Windows networks, Cisco Systems, and Orion SolarWinds. Experience with Zero Trust Architectures and Methodologies is desired; Has one or more of the following certifications aligned with the enterprise deployed network architectures: Security+ and Cisco Certified Network Associate (CCNA) or equivalent (i.e., BCNE for Brocade, etc.).

BACKGROUND: An Automated Data Processing (ADP) sensitivity level determination is required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must have strong oral and written communications skills to effectively present information to a broad audience of Government officials, medical professionals, and highly specialized technical personnel.

JOB TITLE: Systems and Network Specialist (Sembach, Germany)

RESPONSIBILITIES: Provides computer systems maintenance and repair. Maintains servers, software systems and networks. Diagnoses and resolves hardware, software, firmware and network problems. Configures, maintains and upgrades network connection devices, network hardware/software equipment, and automation equipment.

The system and network administrator performs system design for TRICARE Area Office - Europe systems and system components. Maintains, operates, and evaluates desktop, network and communications hardware and software plus the system requirements needed to keep the Local Area Network operational at the indicated percentages. Analyzes ongoing operation of Local Area Network and Wide Area Network system(s) to ensure the hardware and network operating software are functioning properly and operating standards are met. Troubleshoots the Local Area Network, the Wide Area Network, and other network related problems. Coordinates and collaborates with support staff of the host network and all other applicable agencies. Manages, maintains, and supports the development of a standard workstation configuration to be used across all TRICARE Area Office - Europe systems in accordance with Department of Defense and host network regulations. Provides Helpdesk support to on- site users, using available resources to successfully diagnose and resolve problems with desktop computers, laptops, peripherals, commonly used office applications and other information technology as needed. Supports other telecommunication systems as needed, such as telephones, video teleconference systems, etc.

QUALIFICATIONS: Must have a clear understanding of TCP/IP, IPX/SPX, HTTP, SHTTP, SMTP, SNMP, DNS, DHCP, EIGRP, OSPF, PPP, HDLC, V.35, RS-449 and knowledge of the 803.2, 802.3, 802.5, 802.10, 802.11, 802.3u and 802.3z communications, EIA/TIA cable standards and Internet standards. Must address issues related to synchronous and asynchronous communications, Ethernet, Fast Ethernet, Gigabit Ethernet, FDDI, ATM, ISDN, microwave and satellite communications. Required experience with various cable testers and network sniffers.

EXPERIENCE: Possesses understanding of routed, switched and shared LAN environments that operate Microsoft Windows NT/2000, UNIX and OpenVMS and employ various routers switches, hubs and terminal servers as well as various local and long-haul ISDN,56 Kbps through T1 - T3 (European E1 – E3 experience desired), satellite and ATM WAN connectivity that employs Codex and PairGain CSU/DSUs.

EDUCATION: Bachelor’s degree or related technical training in computer science, engineering or information management, or five (5) years related experience and technical certification.

OTHER SKILLS: Experience with DoD Health Care Information Systems is highly recommended. Experience and skills shall include a range of assignments in technical tasks directly related to the proposed area of responsibility. Proficient in Windows networks, Cisco Systems, and Orion SolarWinds. Experience with Zero Trust Architectures and Methodologies is desired; Has one or more of the following certifications aligned with the enterprise deployed network architectures: Security+ and Cisco Certified Network Associate (CCNA) or equivalent (i.e., BCNE for Brocade, etc.).

BACKGROUND: An Automated Data Processing (ADP) sensitivity level determination may be required for this position.

VERBAL & WRITTEN COMMUNICATION SKILLS: Must have strong oral and written communications skills to effectively present information to a broad audience of Government officials, medical professionals, and highly specialized technical personnel.

5.3.1 When using education/certification in conjunction with labor categories, the COR in coordination with the CO must establish a review process of contractor personnel to ensure labor category requirements are met.

PART 6
6.0 INFORMATION TECHNOLOGY & SECURITY

6.1 All work under this contract is considered unclassified. The security requirements are in accordance with the DD Form 254. Key Personnel are required to have and maintain a Secret Clearance. An executed DD254 are required to be part of the contract.

6.2 The TIER 1 or TIER 2 levels and position sensitivity designation for positions under this contract is: (Requirement must be checked in order to be a requirement for this PWS.)

6.2.1 TIER I: Critical sensitive position

6.3 Personally Identifiable Information (PII)/Protected Health Information (PHI), Procurement, and Federal information requirements: Contractor shall comply with Federal Information Requirements for Personally Identifiable Information (PII) and Public Health Information (PHI). Refer to Clause Section for DHA Procedures, Guidance, and Information Part 24 – Protection of Privacy and Freedom of Information PII/PHA and Federal Information Requirement DHA PGI 224.1-90 as applicable.

6.3.1. Data Sharing Agreements (DSAs): Contractors requiring access to PII, which includes PHI, or access to de-identified data, are subject to the DHA Privacy and Civil Liberties Office (DPCLO) (Privacy Office) Data Sharing Program. This program requires DHA to enter into DSAs with parties outside the MHS who use or create MHS data. A DHA contract may use the term Data Use Agreement (DUA) rather than DSA. DSAs assure that outside parties protect MHS data in accordance with the Privacy Act and the HIPAA Rules. To apply for a DSA, the contractor submits a Data Sharing Agreement Application (DSAA) to the DHA DPCLO. The contractor submits the DSAA even if a subcontractor will be the party accessing MHS data. After review and approval of the DSAA, the Privacy Office provides a DSA to the contractor for execution.

6.3.2. Processing Procurement Sensitive Information: All individuals shall seek guidance from the CO regarding the coordination of documents, dissemination, and transmission of procurement sensitive information. Procurement sensitive information shall not be transmitted electronically unless encryption is utilized. Depending on a particular procurement, other restrictions may apply.

6.4 Training

6.4.1 Contractor employees performing cybersecurity/cyberspace functions shall comply with the following requirements:

6.4.1.1 Training: All contractor and associated subcontractor employees working Cybersecurity Information Assurance (IA)/Cyberspace functions must comply with DoD training requirements in Department of Defense Directive (DoDD) 8140.01 and DoD 8570.01-M. Contractors shall identify, document, track, and report qualifications of contract support personnel who perform cyberspace work roles.

6.4.1.2 Certification: The contractor shall ensure that personnel accessing IS have the proper and current IA certification to perform IA functions at contract award in accordance with DoD 8570.01–M, IA Workforce Improvement Program. The contractor shall meet the applicable IA certification requirements as outlined in DFARS 252.239-2001, including:

6.4.1.2.1 DoD-approved IA workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01–M; and

6.4.1.2.2 Appropriate operating system certification for IA technical positions as required by DoD 8570.01–M.

6.4.1.2.2.1 Upon request by the Government, the contractor shall provide documentation supporting the IA certification status of personnel performing IA functions.

6.4.1.2.2.2 Contractor personnel who do not have proper and current certifications shall be denied access to DoD IS for the purpose of performing IA functions.

6.4.2 User requirements: All contractor employees that require access to DHA IT must comply with the requirements of DHA-Procedural Instruction 8140.01, Acceptable Use of DHA IT, to include those contract employees with privileged access.

6.5 Cybersecurity Requirements for Non-DoD IT or Covered Contractor IS:

RESERVED

6.6 Risk Management Framework (RMF) for DoD IT: All IS, Platform Information Technology (PIT) and IT Services or Products under this requirement, that receive, transmit, store, or process nonpublic government data must be accredited in accordance with DoDI 8510.01, Risk Management Framework (RMF) for DoD IT and comply with annual Federal Information Security Modernization Act (FISMA) security control testing. IS and PIT systems must be categorized in accordance with Committee on National Security Systems Instruction (CNSSI) 1253, implement a corresponding set of security controls from the NIST SP 800-53, and use assessment procedures from NIST SP 800-53A with additional DoD-specific assignment values, overlays, implementation guidance, and assessment procedures as required.

6.6.1 All systems subject to RMF must present evidence of authorization in the System Security Plan, Security Assessment Report) a Plan of Action and Milestones (POA&M) and authorization decision document or show that the system has a DoD RMF or equivalent DoD Component PIT system accreditation decision that is current within 3 years within 5 business days of CO request. Evidence of FISMA compliance must be presented in the form of a POA&M. Systems must have and maintain an Authority to Operate (ATO) or Authority to Operate with Conditions (ATO-C) by contract award.

6.6.2 The contractor shall implement security controls in accordance with NIST implementation and validation requirements specified in the NIST SP 800-37 Risk Management Framework (RMF) and DoDI 8510.01, Risk Management Framework (RMF).

6.6.3 The contractor shall configure the information system in accordance with Defense Information Agency (DISA) Security Requirements Guides (SRGs) and security technical implementation guides (STIGs).

6.6.4 The contractor shall ensure that the information system conforms to the requirements of DoDI 8551.01 "Ports, Protocols, and Services Management (PPSM)".

6.6.5 The contractor shall ensure that the information system shall authenticate all entities as specified in DoDI 8520.03 "Identity Authentication for Information Systems" prior to granting access.

6.6.6 The contractor shall Public Key (PK) enable the information system, implementing digital signature and encryption requirements specified in DoDI 8520.02, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling".

6.6.7 The contractor will be responsible for compliance with the Joint Force Head Quarters – Department of Defense Information Network issuances and IA Vulnerability Management (IAVM) issuances by ensuring that the issuances are assessed, implemented and maintained throughout development and sustainment in accordance with specified timelines.

6.6.8 The contractor shall support reciprocity, by providing all directed information in NIST security documents to the government.

6.6.9 The contractor shall implement system level protection and detection capabilities that are consistent with their contract for NIST Security requirements that meet DoD and DHA Cybersecurity Architectures.

6.6.10 Cyber Incident Reporting Requirement: The contractor shall comply with the incident management requirements of Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01B, "Cyber Incident Handling Program".

6.6.11 Information security continuous monitoring (ISCM): ISCM is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. ISCM is a critical part of the risk management process to ensure that IS and PIT operations remain within an acceptable level of risk despite any changes that occur. The Contractor shall maintain ongoing monitoring, analysis and incident response procedures for all ARRT and PIT systems under this requirement in accordance with NIST SP 800-137.

6.6.12 The contractor shall mitigate supply chain risk to the government by complying with DFARS 252.239-7018 and only utilizing unified capability equipment identified on the DODIN

Unified Capabilities Approved Products List (**https://aplits.disa.mil/processAPList**), unless granted a waiver in accordance with DODI 8100.04, DOD Unified Capabilities (UC).

6.7. Facility Related Control Systems: The DHA's Facilities Enterprise (FE) Program Management Office (PMO) establishes the processes for acquisition, installation and sustainment of FRCS in DHA Facilities. Requirements for cybersecurity of FRCS are developed and specified by the FHA FE FRCS PMO. The scope of PIT and Control Systems within the DoD includes building control systems such as Heating Ventilation and Air Conditioning, Utility Management Control System, Electronic Security Systems, Fire Alarm Systems, and other assets. The application of IT cybersecurity strategies is migrating into PIT and Control Systems in response to emerging threats. The requirements within this scope apply to all versions of Design-Build (DB); Design-Bid-Build (DBB); and facilities Sustainment, Restoration and Modernization (SRM) projects as well as Initial Outfitting (IO) requirements activities.

6.7.1 **Applicability:** Contractors shall agree to the DHA Cybersecurity requirements as outlined for those project-specific FRCS Systems selected from Military Standard (MIL-STD) 1691, (*https://home.facilities.health.mil/military-standard-milstd-1691-equipment*) and identified in the DBB design process, D-B RFP development, SRM procurement documentation, or IO requirements unless an exception has been granted for a system by the Government prior to project award or procurement order issuance.

6.7.2 **Cybersecurity Design:** Failure to meet the design requirements may result in Government non-acceptance of submittals or termination of the procurement delivery order for cause, in accordance with project documentation and FAR 52.212-4(m).

6.7.2.1 The contractor shall comply with Unified Facilities Criteria (UFC) 4-010-06 Cybersecurity of Facility-Related Control Systems, UFGS 25-05-11 Cyber Security for Facility-Related Control Systems, and referenced standards to develop a Cybersecurity program for their FRCS products to be installed in DoD facilities. The UFC system is prescribed by MIL-STD 3007 and provides planning, design, construction, sustainment, restoration, and modernization criteria, and applies to the Military Departments, the Defense Agencies, and the DoD Field Activities in accordance with Under Secretary of Defense Acquisition, Technologies, and Logistics Memorandum dated 29 May 2002. UFC will be used for all DoD projects and work for other customers where appropriate.

6.7.2.2 Contractors shall comply with the National Information Assurance Partnership (NIAP) Common Criteria Cybersecurity Evaluation and Validation Scheme (CCEVS) evaluation (*https://www.niap-ccevs.org*) which is published on the NIAP-CCEVS Products Compliance List. The NIAP-certified products have been assessed from a security perspective, helping to reduce the existence of potential vulnerabilities. Contractors are required to continually maintain their products, mitigate vulnerabilities, and distribute fixes to licensed users.

6.7.2.3 The contractor agrees to comply with security regulations and guidance listed in **Attachment 3, Cybersecurity Regulations and Guidance**, and all RMF requirements. The contractor shall establish appropriate administrative and technical safeguards to ensure the confidentiality, integrity, and availability of Government data under their control.

6.7.3 **Funding of FRCS System/Device Requirements:** Projects requiring new or replacement FRCS, or upgrade/extension of existing devices/systems, employ either SRM, DB, or DBB acquisition strategies. Many FRCS are categorized as Real Property and are project funded. Others are categorized through Military Standard 1691 as Personal Property (PP) requiring IO funding. The IO effort should preferably, and where feasible, be embedded in the SRM, DBB or DB contract through Contract Line Items or another vehicle. This will optimize coordination of project-funded infrastructure design/construction with FRCS device/system design, installation, testing and commissioning. Where the project delivery team (PDT) determines that acquisition of PP devices/systems will be through IO action entirely separate to the SRM, DBB, or DB contract, the same RMF-related activities are required. These activities shall be fully integrated into the project master schedule.

6.7.3.1 Pricing for Cybersecurity: If there are any additional costs associated with any element of the Cybersecurity lifecycle including a test/laboratory environment, the Contractor shall provide those costs as follows:

6.7.3.1.1 All costs to assist the Government to achieve a new ATO and maintain it during the equipment's warranty shall be included in the initial quote/offer price for SRM, and in the proposal for DB/DBB projects.

6.7.4 **FRCS Cybersecurity Requirements:** The contractor shall provide a POC responsible for the cybersecurity of the contractor device or system, throughout the lifecycle of the product. The contractor shall provide Subject Matter Experts to support all assessments of contracted products and materials.

6.7.4.1 The contractor shall establish and utilize a test/laboratory environment that duplicates all contractor fielded equipment/product that falls within the FRCS system/device authorization boundary. The contractor shall ensure that all fielded equipment/product is maintained during the construction/installation period of performance, and for fifteen (15) years post acceptance or as long as the contractor commercially supports the equipment/product, whichever is longer.

6.7.4.2 The contractor's test/laboratory environment shall be used to submit to the Government, either through the RFP response, procurement order offer/quote, or construction submittal process, with all sections of the FRCS Risk Assessment Questionnaire and a Nessus vulnerability assessment report.

6.7.4.3 Contractors must provide a fully credentialed Nessus scan of the laboratory environment utilizing the DoD policy template with the submission. In addition, Nessus scans shall be provided within ten (10) days of a request from the Government POC to ensure a continuous monitoring program. Nessus scanner must be procured by the contractor, at their own cost, in order to comply with RMF requirements. The contractor shall request the latest versions through the CO.

6.7.4.4 Contractors shall notify the assigned Government POC FRCS analyst of any updates/changes to the system and attain Government approval from the Military Treatment

Facilities (MTFs) Change Control Board prior to installation. This should include operating system updates/patches; contractor application and database upgrades, updates, and patches; other software/firmware updates/patches; and addition/removal of components.

6.7.4.5 The contractor shall comply with DoDI 8500.01 Cybersecurity, Enclosure 3, paragraph 9.b.(11), requiring all cybersecurity products and IA-enabled products that require use of the product's cybersecurity capabilities will comply with the evaluation and validation requirements of Committee on National Security Systems Policy 11, National Policy Governing the Acquisition of IA and IA-Enabled Information Technology Products, June 2013, as amended.

6.7.4.6 The contractor shall comply with DoDI 8510.01, Enclosure 6, para 2.f(6)(a), ensuring systems must be reassessed for reauthorization prior to the Authorization Termination Date. Government Program Offices or appropriate facilities organizations plan for this activity. The results of an annual cybersecurity review or a negative change to the system or environment at any time (i.e., a change increasing the residual risk) may result in a need for reauthorization prior to the regular three-year reauthorization.

6.7.4.7 If the FRCS is Internet Protocol capable, the proposed system shall be Internet Protocol Version 6 (IPv6) capable or the contractor shall provide a detailed project, migration or planning documentation to show when the proposed system shall be IPv6 capable. The contractor shall be able to demonstrate or provide documentation to prove that their product is IPv6 capable.

6.7.4.7.1 Minimum IPv6 capabilities include:
(a) Conformant with the IPv6 standards profile contained in the DoD IT Standards Registry (DISR);
(b) Maintaining interoperability in heterogeneous environments with IPv4;
(c) Commitment to upgrade as the IPv6 standard evolves;
(d) Availability of contractor IPv6 technical support.

6.7.4.8 The contractor shall notify the Government POC and CO POCs in writing with any inabilities to comply with DoD security requirements. The contractor will provide anticipated costs and timelines required to address any vulnerabilities in question.

6.7.5 **Post Award Requirements:** Contractor provided network infrastructure components (e.g. switches, routers, etc.) shall be standardized to the existing MTF network infrastructure where possible and shall be listed on the DoD Information Network Approved Products List (APL) (*https://aplits.disa.mil*). Operating systems and firmware shall be the most current government approved version approved for infrastructure components, workstations, and servers.

6.7.5.1 As technology requirements change and compliance requirements transition, the contractor shall maintain their solution and incorporate new system/device capabilities and requirements into their proposed design. Contractors should at a minimum provide documentation that details what changes/requirements cannot apply to the current version and provide a schedule when the capabilities will be incorporated into future versions to ensure continued compliance and functionality.

6.7.5.2 The contractor's installed device or system shall pass pre-validation technical screening including fully-credentialed vulnerability scans utilizing Nessus, Security Content Automation Protocol scans, and STIGs checklists within 6 months of construction submittal acceptance, or procurement contract award, and prior to related commissioning activity or acceptance testing. All resulting documentation will be provided by the contractor to the Government POC for review. The contractor shall mitigate or remediate all Very High, High, and Moderate severity vulnerabilities discovered during the RMF Assessment process according to the associated POA&M.

6.7.5.2.1 Successful pre-validation technical screening must meet the Cybersecurity criteria listed below:

(a) No unmitigated Very High or High severity, vulnerabilities as described in the appropriate DISA STIGs located on *https://public.cyber.mil/stigs/*.
(b) No unmitigated Moderate severity, vulnerabilities described in the appropriate DISA STIGs located on *https://public.cyber.mil/stigs/*.
(c) No unmitigated Very High or High severity vulnerabilities from Nessus vulnerability scans.
(d) No unmitigated Moderate severity vulnerabilities from Nessus vulnerability scans.

6.7.5.2.2 The contractor will provide the following documentation on their system/device:

(a) Manufacturer name/model, version, and functionality description
(b) Product specifications
(c) Technology Architecture Diagram (System topology)
(d) Provide Hardware, Software, and Firmware Inventory
(e) Provide Ports Protocols and Services that are required for System functionality
(f) Provide a data flow diagram with detailed topology (include any required interfaces to other Systems)
(g) Complete a DD Form 2930, Privacy Impact Assessment

6.7.5.3 In DBB and DB contracts, the contractor shall submit requests for the templates and any additional technical documentation through the standard RFI process. Completed documents shall be provided to the Government though the standard Submittal process for Government Approval. For SRM projects and IO requirements, the contractor shall submit a request for the templates and any technical documentation within twenty (20) days of contract award. The required schedule for requests and responses is identified in the timeframes below for each acquisition strategy. **Attachment 4, FRCS Responsibility Matrix**, provides a Responsibility Matrix overview of the project roles and responsibilities.

6.7.5.4 For all devices/systems requiring an ATO:
(a) For SRM projects and IO requirements, the contractor shall not make any delivery and shall not receive payment for the until the Government POC has approved the self-assessment of the test/laboratory environment. The contractor must receive written confirmation from the CO that the system/device has successfully completed a self-assessment and that the contractor may proceed with delivery. Delivery may take place prior to this milestone only if written permission is provided by the CO.

(b) For DBB and DB MILCON-funded FRCS, the contractor proceeds at his own risk if the contractor has not received Government approval that the system/device has successfully completed a self-assessment. Once the system/device has been installed, commissioning or acceptance testing shall not proceed until the Government POC, with contractor support and mitigation, has completed a successful self-assessment of the installation, and the Independent Verification & Validation (IV&V) has been scheduled (if required). An IV&V cannot be scheduled until all documentation requirements and technical requirements have been completed to the Government POC's satisfaction. Additionally, all required POA&Ms must have been identified, and been appropriately mitigated to reduce the risk to the Government network and PHI/PII/For Official Use Only data housed within the system.

6.7.5.5 A contractor's technical solution that requires an Assessment and Authorization shall be able obtains a recommendation of ATO from a Government-appointed third-party validator within twelve (12) months of the successful installation self-assessment.

6.7.6 **Cybersecurity Assessment:** The contractor's solutions shall be configured to allow Endpoint protection, allow unattended credentialed scans, and allow patching without contractor intervention.

6.7.6.1 The contractor solution shall comply with DoD Instruction 8582.01, "Security of Non-DoD Information Systems Processing Unclassified NonPublic DoD Information. Devices and systems must be configured in such a way that allows the updating of malware definition signatures on a scheduled basis. Scanning shall encompass the entire system (file system, operating system, and real-time processes) by default. In cases where scanning of the entire system may negatively affect its operation, the contractor shall provide a detailed list of exclusions with justifications. The contractor shall provide technical specifications that clearly demonstrate whether the proposed solution can integrate and support either the full security suite or the individual components (e.g. Data Loss Prevention, Intrusion Prevention System, Antivirus, etc.) without performance degradation of the contractor device or system. In cases where the operation of security applications is not technically achievable, the contractor shall provide detailed justification and a POA&M describing steps towards mitigations or compliance with this requirement.

6.7.6.2 The contractor shall ensure that the selected FRCS system/device is capable of supporting configuration control allowing the FRCS to be fully managed and controlled at a local level, without contractor or manufacturer approval. Specifically stating that patch management activities, vulnerability management, security updates, STIG hardening, etc. are able to be conducted without contractor intervention. FRCS that requires contractor intervention, outside of an approved Business-2-Business (B2B) connection, does not meet the requirement for this section. In cases where Configuration control of the system/device may negatively affect its operation, the contractor shall provide a detailed list of exclusions with justifications. The contractor shall provide technical specifications that clearly demonstrate whether the proposed solution can support the Configuration control without performance degradation of the contractor device or System. In cases where the operation of security applications is not technically

achievable, the contractor shall provide detailed justification and a POA&M describing steps towards mitigations or compliance with this requirement

6.7.6.4 The contractor shall submit all RMF-required documentation for review and approval per the Assessment Timeline in paragraph 6.7.7.

6.7.6.5 The contractor shall obtain approval from the Government for any contractor developed RMF policies, plans, and procedures, prior to implementation.

6.7.6.6 The contractor shall provide any additional documentation required by the Government for completion of the assessment process within thirty (30) business days of a request by the Government.

6.7.6.7 The contractor shall provide technical scans per the Assessment Timeline below.

6.7.6.8 The contractor shall provide updated Nessus scans within ten (10) days of a request from the Government POC until an ATO is granted or the product is added to the DHA FE APL.

6.7.6.9 The contractor shall remediate or mitigate any findings discovered as a result of the Nessus scans.

6.7.7. **Risk Assessment Timeframes:** Each acquisition strategy has a different cycle of design and procurement for FRCS which generate different schedules and timelines for RMF-related activities. These timelines may also be impacted by local or programmatic requirements. Consequently, the schedules included in **Attachment 5, Risk Assessment Timeframes** are to be considered as templates and should be reviewed and modified where necessary by the PDT for a specific project, as they develop procurement documents, scopes of work, performance work statements, RFPs, Specifications, etc.

6.7.7.1 Where the PDT determines that acquisition of PP devices/Systems will be through IO action entirely separate to the SRM, DBB, or DB contract, the same RMF-related activities are required. These activities in Part 8 shall be fully integrated into the project master schedule.

6.7.8 **Warranty and Post-Warranty Service Maintenance Agreement:** The contractor shall maintain all equipment/product versions provided pursuant to the construction or other procurement contract, to include the supported operating system, by issuing patches/updates to mitigate vulnerabilities [e.g., IAVA or IA Vulnerability Bulletins (IAVB)] and network security configurations [e.g., Defense Information System Agency (DISA) STIGs]. The contractor must adhere to DHA guidance for remediation or mitigation of vulnerabilities associated with the equipment/product.

6.7.8.1 Contractors shall be responsible for providing cybersecurity maintenance support for as long as the contractor commercially supports the system/device or fifteen (15) years after end of sale date of the equipment provided by the contractor. If required, the contractor shall use the Government-approved method for remote access administration (DHA B2B) of the system or device.

6.7.8.2 Pursuant to warranty periods and Service Maintenance Agreements (SMAs), the contractor shall, after the issuance of an ATO or APL approval, ensure that the contractor's device or system maintains its ATO or operating system platform and patches/updates for as long as the contractor commercially supports the system/device or fifteen (15) years after end of sale date of the equipment provided by the contractor.

6.7.8.3 The contractor shall maintain an ATO or APL approval on all equipment/product versions owned by the HA) and Services and originally purchased through the contractor's contract. If a contractor cannot support the ATO or APL approval for all DHA/Service owned versions of the equipment/product, the contractor can meet this requirement by offering to provide all upgrades to the equipment/product that are required to maintain the ATO or APL approval, either at no cost to the Government or at a fixed price that is included in a RMF only maintenance offering under the contractors contract. During the period of time the contractor has a product installed on the network, the contractor shall provide all required cybersecurity patches/updates. Maintaining the RMF ATO or APL approval shall be included as part of the contractor's warranty period. For updates/patches, executable files should be distributed by the manufacturer accordingly, or implemented by the manufacturer's technical staff, dependent on the Service Agreement processes.

6.7.8.4 The contractor shall notify the PMO and Contracting Officer POCs in writing with any inabilities to comply with DoD security maintenance requirements. Contractor will provide anticipated costs and timelines required to address any vulnerabilities in question.

6.7.9 **Cybersecurity Requirements/Continuous Monitoring/Risk Management**

6.7.9.1 Utilizing a test/laboratory environment, the contractor shall be able to duplicate all fielded equipment/product that falls under the authorization boundary. The contractor shall maintain the system or device in an operational condition with the latest security patches installed.

6.7.9.2 The contractor shall ensure that all fielded equipment/product falling under one authorization is tested to maintain the ATO or approved. For each version owned by DHA and originally purchased through the contractor's contract, the contractor will ensure that each component within the authorization boundary is represented in the test/laboratory group.

6.7.9.3 The contractor shall continually monitor the authorized security configuration and notify the government within forty-eight (48) continuous hours of any new vulnerabilities discovered either in the laboratory or production environments.

6.7.9.4 The contractor shall test all IAVAs, patches, updates, and upgrades in the test/laboratory environment before implementing in a production environment. All production environment IAVAs, patches, updates, and upgrades will be approved by the MTF's Change Control Board prior to contractor implementation. Approved changes shall be implemented on a quarterly basis.

6.7.9.5 The contractor shall review all required policies, plans, and procedures documentation on an annual basis and submit changes to Government for approval.

6.7.9.6 The contractor shall ensure the contractor's device or system is in compliance with the DoD IAVM program upon each additional deployment.

6.7.9.7 The contractor shall monitor the public DoD Cyber Exchange website for new or updated STIGs. The contractor shall implement updated STIG compliance for systems or devices within three (3) months of their availability on the DoD Cyber Exchange.

6.7.9.8 A major upgrade such as major software or hardware revision must be reassessed for ATO or addition to the APL. Minor upgrades must be assessed by the Government to determine if a reauthorization is required. The contractor shall support reauthorizations due to both major and minor upgrades.

6.7.9.9 The contractor shall update all ATO or approved products required supporting documentation in the event of a system policy, procedural, logical or technical changes to the system or device.

6.7.9.10 The contractor shall provide vulnerability and configuration scan results of the test/laboratory environment to the Government on a quarterly basis. The contractor shall provide raw scan results and administrative reports no later than ten (10) calendar days after a request from the Government POC.

6.7.9.11 The contractor shall close all discovered vulnerabilities within three (3) months of discovery or provide a POA&M describing how they will work to close the vulnerability.

6.7.9.12 The contractor shall submit to the Government for approval, all mitigation plans that address any open vulnerabilities.

6.7.9.13 The contractor shall ensure any new deployment (including rebuilds) deploy with a fully patched, accredited version maintained in a lab environment.

6.7.9.14 The contractor shall make the test/laboratory system available for periodic security reviews, within forty-five (45) business days of notification by Government. The contractor shall perform monthly vulnerability scans using the most recent and updated version of approved DoD scan tools.

6.8. System Communications

RESERVED

6.9 MHS Demilitarized Zone (DMZ) Medical Community of Interest (MedCOI) Business-to-Business (B2B) Gateway

6.9.1 If there is an external system connection to a DoD IS required, then the contractor shall, in accordance with contract requirements, connect to the DHA B2B Gateway via a contractor procured Internet Service Provider (ISP) connection.

6.9.2 The contractor shall assume all responsibilities for establishing and maintaining their connectivity to the B2B Gateway. This shall include acquiring and maintaining the circuit used to connect to the B2B Gateway and the acquisition of a Virtual Private Network (VPN) device maintenance agreement and license compatible with the MHS VPN device. The list of compatible devices are detailed in the DHA B2B/MedCOI Gateway questionnaire.

6.9.3 The contractor shall submit a completed current version of the DHA B2B Gateway questionnaire to their Contracting Officer or COR within 10 calendar days after new requirements have been provided to the contractor.

6.9.4 The contractor shall provide information specific to their connectivity requirements, proposed path for the connection and last mile diagram.

6.10 Contractor Provided IT Infrastructure

6.10.1 Platforms shall support HyperText Transfer (Transport) Protocol (HTTP), HyperText Transfer (Transport) Protocol Secure (HTTPS), web-derived Java Applets, and Secure File Transfer Protocols (SFTPs) (e.g., STFP, Secure Socket Layer/Transport Layer Security), and all software that the contractor proposes to use to interconnect with DoD facilities.

6.10.2 The contractor shall configure their networks to support access to Government systems (e.g., configure ports and protocols for access).

6.10.3 The contractor shall provide full time connections to a TIER 1 or TIER 2 ISP. Dial-up ISP connections are not acceptable. All IP addresses need to be publicly routable. Private address space using Network Address Translation will not be permitted.

6.10.4 The contractor shall maintain a valid maintenance contract and pertinent licenses for all devices connecting to the MHS B2B Gateway.

6.11 System Authorization Access Request (SAAR), Defense Department (DD) Form 2875

6.11.1 The contractor shall submit the most current version of DD Form 2875, “System Authorization Access Request (SAAR), in accordance with CO guidance for all contractors that use the DoD Gateways to access Government IT systems and/or DoD applications shall. A DD Form 2875 shall be completed for each contractor employee who will access any system and/or application on a DoD network. The DD Form 2875 shall clearly specify the system and/or application name and justification for access to that system and/or application.

6.11.2 The contractor shall submit the completed DD Form 2875 to the DHA IT Security for verification of Tier I or Tier II Designation. The DHA Personnel Security will verify that the contractor employee has the appropriate background investigation completed or a request for

background investigation has been submitted to the Office of Personal Management (OPM). Acknowledgment from OPM that the request for a background investigation has been received and that an investigation has been scheduled will be verified by the DHA Personnel Security prior to access being approved.

6.11.3 Upon approval, DHA will notify the user of the ID and password via secure/encrypted e-mail upon the establishment of a user account. User accounts will be established for individual use and may not be shared by multiple users or for system generated access to any DoD application. Misuse of user accounts by individuals or contractor entities will result in termination of system access for the individual user account.

6.11.4 The contractor shall conduct a monthly review of all contractor employees who have been granted access to DoD IS'/networks to verify that continued access is required

6.11.5 The contractor shall provide the DHA DPCLO with a report of the findings of their review by the 10th day of each month following the review. Reports identifying changes to contractor employee access requirements shall include the name, DoD ID number from CAC, Company, IS/network for which access is no longer required and the date access will be terminated.

6.12 MHS Systems Telecommunications

6.12.1 The primary communication links shall be via encrypted tunnels (i.e., Secure Internet Protocol (IPSEC), GetVPN, or Secure Socket Layer) between the contractor's primary site and the MHS B2B Gateway.

6.12.2 The contractor shall place the VPN appliance device outside the contractor's firewalls and shall allow full management access to this device (e.g., in router access control lists) to allow Central VPN Management services provided by DHA or other source of service as designated by the MHS to remotely manage, configure, and support this VPN device as part of the MHS VPN domain.

6.12.3 The contractor shall procure and configure for operation an auxiliary VPN device for backup purposes to minimize any downtime associated with problems of the primary VPN.

6.12.4 The contractor shall send devices to the MHS VPN management authority (e.g., DHA) via postage paid and include prepaid return shipping arrangements for the devices(s).

6.12.5 The MHS VPN management authority (e.g., DHA) will remotely configure and manage the VPN appliance once installed by the contractor.

6.12.6 The contractor shall be responsible for the maintenance and repair of contractor procured VPN equipment.

6.12.7 The Government will be responsible for the troubleshooting of VPN equipment.

6.13 Establishment of Telecommunications

6.13.1 Telecommunications shall be established with the MHS through coordination with DHA.

6.13.2 The contractor and DHA Program Office shall identify their requirement(s) for the establishment of telecommunications with the MHS and/or other Government entities.

6.13.3 The DHA/MedCOI B2B Gateway Questionnaire (provided by DHA) identifies the required telecommunication infrastructure between the contractor and the MHS systems. This includes all Wide Area Network, Local Area Network, VPN, Web DMZ, and B2B Gateway access requirements.

6.13.4 The contractor shall complete their applicable portion of the questionnaire and shall return it to the DHA designated POC for review and approval.

6.13.5 The contractor shall, upon Government request, provide technical experts to provide any clarification of information provided in the questionnaire. DHA will review and process the questionnaire when it is accepted.

6.13.6 DHA will coordinate any requirements for additional information with the POC and schedule any meetings required to review the Questionnaire. Upon approval of the Questionnaire, DHA will coordinate a testing meeting with appropriate stakeholders.

6.13.7 DHA will notify the contractor POC of the meeting schedule. The purpose of the testing meeting is to complete a final review of the telecommunication requirements and establish testing dates.

6.14 Contractors Located On Military Installations

6.14.1 The contractor(s) shall coordinate/obtain the connections with the local MTFs/ Enhanced Multi-Service Markets (eMSMs) and Base/Post/Camp communication personnel located on a military installation who require direct access to Government systems.

6.14.2 These connections will be furnished by the Government.

6.14.3 Contractors located on military installations that require direct connections to their networks shall provide an isolated IT infrastructure. They shall coordinate with the Base/Post/Camp communications personnel and the MTF/eMSM in order to get approval for a contractor procured circuit prior to installation to ensure the contractor is within compliance with the respective organizational security policies, guidance and protocols.

Note: In some cases, the contractor may not be allowed to establish these connections due to local administrative/security requirements.

6.14.4 The contractor shall be responsible for all security certification documentation as required to support DoD IA requirements for network interconnections.

6.14.5 The contractor shall provide, on request, detailed network configuration diagrams to support IA accreditation requirements.

6.14.6 The contractor shall comply with IA accreditation requirements. All network traffic shall be via Transmission Control Protocol/Internet Protocol using ports and protocols in accordance with current Service security policy. All traffic that traverses MHS and/or military Service Base/Post/Camp security infrastructure is subject to monitoring by security staff using Intrusion Detection Systems.

DODIN Decision Tree_160929.pptx

PART 7
7.0 ATTACHMENTS/TECHNICAL EXHIBIT LISTING

7.1 The following forms are to be completed by the FSO/Security POC, or COR once the contractor is granted the proper background investigation.

7.1.1 Contractor CAC Request Process


DHA CAC Request Process.pdf


DMDC TASS Application.xlsx

7.1.2 DHA's contractor training instructions


DHA FY22 Annual Training List_Oct 2021

7.1.3 DHA's new employee handbook


DHA CAE (J-4) New Employee Handbool

PART 7, ATTACHMENT 1
PERFORMANCE REQUIREMENTS SUMMARY (PRS)

The contractor service requirements are summarized into performance objectives that relate directly to mission essential items. The performance threshold briefly describes the minimum acceptable levels of service required for each requirement. These thresholds are critical to mission success.

Performance Objective	PWS Reference	Acceptable Quality Level (AQL) (This is the maximum error rate.	Method of Surveillance
PRS# 1. The contractor shall provide Complete Reports.	Reports submitted as required in 4.5 & 4.6	Not more than 5% late	Monthly check of submission logs
PRS # 2 Provide problem diagnosis and resolution	Responses are accurate, current and tailored to the individual needs of the caller and to the MTF	Receive no more than three valid complaints about service during the month	Customer Complaints
PRS # 3 Maintain network Equipment	Equipment failures, non-availability or maintenance shall not interfere with MTF operations	Equipment failures, non-availability or maintenance do not interfere with MTF operations for more than 72 hours during a month	Customer Complaints; Random Inspections
PRS # 4 Dispose of excess equipment	Equipment that is at the end of its lifecycle or is otherwise excess or unusable will be turned in or disposed per Government direction in a timely manner	Excess equipment will be turned in or disposed of within 7 workdays of identification	Random inspection, valid receipts from Tobyhanna or other disposal facilities
PRS # 5 Satisfy Customer	Semi-annual Customer Satisfaction Surveys report satisfactory or Better performance	Survey results of not less than average of 3 on 5-point Likert Scale for 12-month period	Reported to TM with Monthly Progress Report

PRS # 6 Perform Inventory	Semi-annual inventory report accurately reflects all existing network infrastructure equipment and contains the information required by 2.2.3	Inventory contains all Required information, is 95% accurate, includes each site with no more than two sites missing deadline by no more than 15 days	Random inspections
PRS # 7 Vulnerability Management: Patching Compliance Rate	Percentage of network devices (Core Switches, Distro Switches, Edge Switches, Servers, etc) that are patched within the specified timeframe	95% of critical patches applied within 48 to 72 hours of release by DHA Ref: 6.7.6	Monthly Progress Report
PRS # 8 Report Vulnerability Remediation Time	Average time to remediate identified critical/high vulnerabilities	Within 7 days after identification of vulnerability Ref: 6.7.6	Reported directly to TM when identified, and when remediated
PRS # 9 Resolve all High/Critical Vulnerabilities	Number of Unresolved High/Critical Vulnerabilities	Target is zero, or below a predefined threshold 6.7.6	Reported to TM with Monthly Progress Report
PRS # 10 Security Incident Management: Mean Time to Detect (MTTD) Security Incidents	Average time from incident occurrence to detection	< 30 minutes for critical incidents 6.7.6	Reported to TM with Monthly Progress Report
PRS # 11 Mean Time to Respond (MTTR) to Security Incidents	Average time from detection to initial containment/response	< 1 hour for critical incidents	Reported to TM with Monthly Progress Report
PRS # 12 Mean Time to Resolve (MTTR) Security Incidents	Average time from detection to full resolution	< 4 hours for critical incidents	Monthly Progress Report
PRS # 13 Report number of Security Incidents by severity	Number of Security Incidents by severity	Target is zero, or decreasing trend month over month	Monthly Progress Report

PRS # 14 Access Control: Regular Access Review Compliance	Percentage of user access reviews completed on schedule	100% quarterly, with percentage complete reported monthly 6.4.2	Monthly Progress Report
PRS # 15 Report unauthorized access attempts	Number of Unauthorized Access Attempts Blocked (Indicates effectiveness of access controls)	Number of blocked unauthorized access attempts reported monthly 6.4.2	Monthly Progress Report
PRS # 16 Security Audits & Compliance: Perform Audits	Audit Findings Remediation Rate: Percentage of security audit findings remediated within the agreed timeframe	Target: 100% remediation within agreed timeframe; percentage of remediation reported monthly Ref: 6.5.12	Monthly Progress Report
PRS #17 Perform assessments to ensure compliance with Security Policies/Standards	Regular assessments to ensure adherence	100% adherence to defined security baseline configurations is required Ref: 6.5.12	Monthly Progress Report
PRS #18 Ticket Accuracy	Regular and reoccurring assessments to ensure adherence and accuracy.	Target is above 98% accuracy, including tracking of time spent per ticket. Ref: 5.2.3.1	Monthly Progress Report

7.2 OTHER ATTACHMENTS

Attachment 2

RESERVED

Attachment 3, Cybersecurity Regulations and Guidance (Paragraph 6.7.2.3)

Attachment
3-Cybersecurity Regu

Attachment 4, FRCS Responsibility Matrix (Paragraph 6.7.5.3)

Attachment 4-FRCS
Responsibility Matrix.

Attachment 5, Risk Assessment Timeframes (Paragraph 6.7.7)

Attachment 5-Risk
Assessment Timefram

PART 7, ATTACHMENT 6
ESTIMATED WORKLOAD DATA AND CURRENT SITE INFORMATION

Contractors are expected to deliver comprehensive network support and solutions tailored to meet the demands of the current environment. Note: The information provided below is accurate as of 2024, however it is subject to change in response to the network demands of the ecosystem.

- Current sites with on-site contract network support – 102 locations
- Current total sites – 137 MTFs, over 500 Geographically Separated Units (GSUs), and related activities
- Current user population – approximately 179,000
- Current LAN vendors – Brocade, Juniper, and Cisco
- Current network monitoring software – SolarWinds NPM
- Current ITSM software – ServiceNow
- Current logging software – Splunk
- Current comply-to-connect- Cisco ISE

PART 7, ATTACHMENT 7
LIST OF SITES AND ASSOCIATED SUPPORT DETAILS

DHA Site List 2024.xlsx

PART 7, TECHNICAL EXHIBIT 1
DELIVERABLES SCHEDULE

Deliverable	Frequency	Medium/Format	Submit To	Applicable to:
CDRL A001 – Quality Control Plan  CDRL 1 Quality Plan	Within 30 days of award	Contractors discretion	KO	All, See PWS 1.10.1
CDRL A002 - Transition-in, Transition-out CDRLs if a Government requirement for this contract.	Transition-in: Within 30 days of award Transition-out: 6 months prior to close of contract or unexercised option.	Contractors discretion	COR, Alt COR, COR's PM	1.6.1.1 and 1.6.1.2.

Deliverable	Frequency	Medium/Format	Submit To	Applicable to:
CDRL A003 -Non-Disclosure Agreement	Signed statements are due, from each employee assigned, prior to performing ANY work on this task.	Contractors discretion	COR, Alt COR, COR's PM	1.14.2
CDRL A004- Weekly Vacancy Report	Weekly – specific day, as defined by COR	Contractors discretion	COR, Alt COR, COR's PM	1.14.5
CDRL A005 - Monthly Progress Report	With Invoice	Same as above	Same as above	1.14.6
CDRL A006 - Contractor Manpower Reporting	NLT 31 October of each Fiscal Year	Same as above	Same as above	1.14.1
CDRL A007 Program Management Plan	Extended from previous order Updated as required	Same as above	Same as above	5.1
CDRL A008 - Contingency Operations Plan	Updated quarterly	Same as above	Same as above	1.10.3
CDRL A009 - Overseas Housing Allowance Reimbursement Validation/Revalidation Report	Quarterly	Same as above	Same as above	1.9
CDRL A010 – Monthly Inventory of equipment	With Invoice	Contractors discretion	COR, Alt COR, COR's PM, and CO via the PIEE System	5.2.2.1