Department of Defense

Defense Health Agency

Performance Work Statement

Electronic Security System (ESS) Modernization

Directorate for Administration, Operations Management

Naval Hospital Bremerton (NHB)

DRAFT

Solicitation Number: [TBD]

Version: 1.0

Date: June 2026

PART 1

1.0 GENERAL INFORMATION

1.1 This is a non-personal services contract to provide a comprehensive upgrade and potential replacement of the Electronic Security System (ESS) at Naval Hospital Bremerton (NHB).

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 the design, installation, and testing of the ESS 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 and all referenced publications in Section 2.3 of this PWS.

1.3 **Background:** The current security surveillance and detection system at NHB is not compliant with the most current versions of the applicable publications prescribed in Section 2.3 of the PWS. Therefore, this contract is required to modernize the ESS to protect assets—people, facilities, sensitive information, and equipment—thereby supporting the mission of Defense Health Agency (DHA) and NHB.

1.4 **Objectives:** The objectives of this contract are to:

- Provide NHB with a fully functional, reliable, and integrated ESS (Video Surveillance Systems (VSS), Access Control System (ACS), and Intrusion Detection System (IDS)) that meets all requirements referenced in the publications identified in Section 2.3 of this PWS.
- Ensure all required areas of the hospital are under appropriate camera surveillance with adequate video recording and storage capabilities.
- Implement a standalone, cyber-secure system capable of achieving a DoD Risk Management Framework (RMF) Authority to Operate (ATO).

1.5 **Scope:** The Contractor shall provide all necessary program management, engineering, labor, materials, equipment, and supervision to design, procure, install, configure, test, and accredit a complete and operational ESS at NHB, which is compliant with the most current versions of the publications in Section 2.3 of this PWS. The scope includes the full integration of all subsystems, achieving a DoD Authority to Operate (ATO), providing comprehensive training to government personnel, and delivering complete system documentation. The Contractor shall also provide warranty and ongoing maintenance support as defined herein. The final system shall be a standalone network, not connected to the existing hospital network.

1.6 **Period of Performance (PoP):** [To be determined at contract award].

DRAFT

1.7 **Administrative specifications**

1.7.1 Place of performance: The work shall be performed at Naval Hospital Bremerton (NHB) in Bremerton, WA.

1.7.2 Recognized Federal holidays: The Contractor is not required to perform services on Federal holidays.

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.

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 RESERVED.

1.9 RESERVED.

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 Contractor shall prepare and submit its comprehensive QCP within 7 days after contract award to the Government IAW CDRL A001. After acceptance of the Quality Control Plan (QCP) the Contractor shall receive the CO's acceptance in writing of any proposed change to his QC system. See Part 7, Technical Exhibit 1 - 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).

1.11 RESERVED.

1.12 Key personnel (Contractor): 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 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 8:00 a.m. to 4:30 p.m., Monday thru Friday except Federal holidays or when the government facility is closed for administrative reasons.

1.13 RESERVED.

DRAFT

1.14 **Reporting**

1.14.1 RESERVED.

1.14.2 RESERVED.

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. 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.

1.15 **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.

DRAFT

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.

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

1.16.1. Contractor access to the HA/DHA network is contingent strictly on the approved Course of Action (COA) selected by the Government for this effort and subsequent contract award. Specifically, if the proposed ESS is fully Risk Management Framework (RMF) accredited, the Contractor may be granted access to the main HA/DHA network to perform integration, configuration, and testing, subject to final Government approval and compliance with DHA cybersecurity policies. However, if the proposed ESS is not RMF accredited, the Contractor will not be granted access to the main HA/DHA network, and must design, install, and configure the ESS on a completely standalone network infrastructure that maintains total physical and logical separation from the existing hospital network.

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.

DRAFT

DRAFT

PART 2

2.0 DEFINITIONS, ACRONYMS, AND APPLICABLE PUBLICATIONS

2.1 Definitions:

- **Contracting Officer (CO):** A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.
- **Contracting Officer's Representative (COR):** An individual 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.
- **Electronic Security System (ESS):** An integrated electronic system that encompasses Access Control Systems (ACS), Intrusion Detection Systems (IDS), and Video Surveillance Systems (VSS).
- **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.
- **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:

- **ACS** - Access Control System
- **ATO** - Authority to Operate
- **CDRL** – Contract Data Requirements List
- **DoD** - Department of Defense
- **ESS** - Electronic Security System
- **IDS** - Intrusion Detection System
- **NHB** - Naval Hospital Bremerton
- **PWS** - Performance Work Statement
- **RMF** - Risk Management Framework
- **STIG** - Security Technical Implementation Guide
- **UFC** - Unified Facilities Criteria
- **VSS** - Video Surveillance System

2.3 Applicable Publications:

- Committee on National Security Systems Instruction (CNSSI) 1253
- DoDI 2000.16, DoD Antiterrorism (AT) Standards

DRAFT

- DoDI 8510.01, Risk Management Framework (RMF) for DoD IT
- Federal Information Processing Standards (FIPS) Publication 201, "Personal Identity Verification (PIV) of Federal Employees and Contractors"
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- National Fire Protection Association (NFPA) Codes (70, 72, 101)

UFC 4-010-01, “DoD Minimum Antiterrorism Standards for Buildings"

- UFC 4-010-06, "Cybersecurity of Facility-Related Control Systems"
- UFC 4-021-01, "Mass Notification Systems"
- UFC 4-021-02, "Electronic Security Systems"
- UFC 4-510-01, "Design: Military Medical Facilities"

DRAFT

PART 3

3.0 GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

3.1 **Services:** The Government will NOT provide Government Furnished Services in support of this contract.

3.2 **Facilities**: The Government will provide Government Furnished Services required in support of this contract. This includes access to the facility and existing infrastructure pathways (e.g., conduit and cable trays) where feasible. Specific server room space will be designated for new head-end equipment.

3.3 **Utilities:** The Government will provide utilities in support of this contract. 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.

3.5 **Materials:** The Government will NOT provide materials in support of this contract.

DRAFT

PART 4

4.0 CONTRACTOR FURNISHED ITEMS AND SERVICES

4.1 General: The Contractor shall furnish all supplies, equipment, facilities, and services required to perform work listed under Section 5 of this PWS. This includes all cameras, servers, switches, workstations, software, licensing, cabling, and mounting hardware necessary to deliver a complete and operational system.

DRAFT

PART 5

5.0 SPECIFIC TASKS

5.1 Technical Requirements

5.1.1 The Contractor shall deliver a fully functional and integrated ESS for NHB, which is compliant with the applicable publications in Section 2.3 of this PWS.

5.2 General System Requirements

5.2.1 Operational Availability: The Contractor shall ensure the entire ESS achieves a minimum operational availability of 100%, measured monthly. The system shall be supported by an uninterruptible power supply (UPS) to ensure continuous operation for a minimum of two hours during a power outage.

5.2.2 System Latency: The Contractor shall ensure the time delay between sensor activation and annunciation at the operator workstation does not exceed 10 seconds, with a goal of 3 to 5 seconds.

5.2.3 Scalability: The Contractor shall ensure the ESS has a modular architecture capable of supporting a 25% expansion in connected devices through software configuration with minimal hardware additions.

5.2.4 Force Protection Condition (FPCON) Support: The Contractor shall configure the ESS to support all FPCON levels, allowing an administrator to implement progressively stricter security protocols with a single command.

5.2.5 Mass Notification System (MNS) Integration: The contractor shall fully integrate the ESS with the facility's MNS in accordance with UFC 4-021-01. The integration shall support activation via supervised inputs, prioritized messaging (with active shooter taking precedence over fire), pre-recorded messages for all required scenarios, and live voice override.

5.3 **Central Security Management System (SMS) / PSIM Requirements**

The Contractor shall provide a central management platform that provides a single, cohesive interface for operating all integrated subsystems.

5.3.1 Graphical User Interface (GUI): The Contractor shall provide a GUI that displays all system components as dynamic icons on multi-layered facility maps, providing real-time status and intuitive control.

5.3.2 Alarm Annunciation and Workflow: The Contractor shall configure the system to prioritize alarms and automatically execute pre-defined Standard Operating Procedures

DRAFT

(SOPs), presenting operators with step-by-step response checklists and associated video upon an alarm.

5.3.3 System Health Monitoring: The Contractor shall ensure the SMS continuously monitors the health of all system components and generates automated "trouble" alerts to administrators upon detecting a failure or communication loss.

5.3.4 Reporting and Logging: The Contractor shall provide a system capable of generating on-demand and scheduled reports. All operator actions must be logged in a secure, tamper-proof audit trail.

5.4 **Intrusion Detection System (IDS) Performance**

5.4.1 Probability of Detection (Pd): The Contractor shall ensure all IDS sensors have a Pd of at least 95% for specified threats.

5.4.2 Nuisance and False Alarm Rates (NAR/FAR): The Contractor shall ensure the system does not exceed a NAR of three alarms per month for interior sensors and three alarms per day for exterior sensors, and a FAR of one alarm per month for interior sensors and one alarm per day for exterior sensors.

5.5 **Access Control System (ACS) Performance**

5.5.1 Credentialing: The Contractor shall ensure the ACS is FIPS 201 compliant and uses the DoD Common Access Card (CAC) as the primary credential.

5.5.2 Monitoring and Logging: The Contractor shall install Door Position Switches (DPS) on every controlled door and configure the system to generate and log alarms for "forced entry" and "door held open" events. All access events must be logged to create a complete audit trail.

5.5.3 High-Risk Area Control: The Contractor shall implement stringent access control for high-risk areas, including the pharmacy, medical supply storage, laboratories, and data centers.

5.6 **Video Surveillance System (VSS) Performance**

5.6.1 Image Quality: The Contractor shall provide cameras with a minimum resolution of HD 1080p and frame rates appropriate for the monitored scene, sufficient to meet specified detection, recognition, and identification goals.

5.6.2 Alarm Assessment: The Contractor shall configure the VSS to automatically display video from relevant cameras on the operator's monitor upon any IDS or ACS alarm.

5.6.3 Video Storage: The Contractor shall provide Network Video Recorders (NVRs) with sufficient capacity to retain all video for a minimum of 30 days of continuous recording.

DRAFT

5.6.4 Patient Privacy: The Contractor shall ensure camera placement is planned to monitor critical areas while respecting patient privacy and avoiding placement in patient rooms.

5.7 **Installation, Testing, and Training**

5.7.1 Installation: The Contractor shall perform all installation work in a professional manner, adhering to all applicable codes and standards.

5.7.2 System Acceptance Testing (SAT): The Contractor shall execute a government-witnessed SAT to demonstrate that 100% of the system's functions meet PWS requirements.

5.7.3 Training: The Contractor shall provide comprehensive training courses for ESS operators, administrators, and maintenance personnel on-site at NHB beginning at contract award and annually thereafter. As such, the Contractor shall prepare and deliver a training plan and materials to the Government in accordance with CDRL A002.

5.7.4 ESS Documentation: The Contractor shall deliver all “as-built” drawings, user manuals, and maintenance procedures for the ESS to the Government in accordance with CDRL A003.

5.8 **Warranty**

5.8.1 Warranty: The Contractor shall provide a minimum one-year warranty on all parts, labor, and software, commencing upon final government acceptance.

DRAFT

PART 6

6.0 INFORMATION TECHNOLOGY & SECURITY

6.1 All work under this contract is unclassified.

6.2 The TIER 1 or TIER 2 levels and position sensitivity designation for positions under this contract is:

6.2.1 TIER II: Non-critical sensitive position.

6.3 **Personally Identifiable Information (PII)/Protected Health Information (PHI), Procurement, and Federal information requirements:**

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: RESERVED.**

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

6.5.1 The Contractor shall, at time of award, have implemented the security requirements prescribed in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171), in accordance with DFARS clause 252.204-7012.

DRAFT

6.5.2 NIST SP 800-171 DoD Assessment Methodology. The DFARS provision 252.204-7019 introduces the "NIST SP 800-171 DoD Assessment Methodology" requirement. This requirement enables a strategic assessment of a Contractor's implementation of the NIST SP 800-171 requirements as required in DFARS clause 252.204-7012. The DoD Assessment Methodology requirement flows down to subcontractors.

6.5.2.1 Basic Assessment: The Contractor shall obtain and maintain access to the Supplier Performance Risk System (SPRS) via the PIEE, (available via the internet at https://www.sprs.csd.disa.mil/)

6.5.2.1.1 The Contractor shall perform a Basic Assessment, using the NIST SP 800-171 DoD Assessment Scoring Template, and enter the results electronically in SPRS for each covered Contractor information system that is relevant to an offer, contract, task order, or delivery order. **See Attachment 2, Deliverable Schedule Table.**

6.5.2.1.2 The Contractor shall ensure that applicable subcontractors also have their results of a current assessment posted in SPRS prior to awarding a subcontract or other contractual instrument in accordance with DFARS clause 252.204-7020.

6.5.3 The Contractor shall provide the government with access to its facilities, systems, and personnel when necessary to conduct or renew a higher-level (i.e., Medium or High) assessment in accordance with DFARS clause 252.204-7020.

6.5.4 Cybersecurity Maturity Model Certification (CMMC): The CMMC (DFARS clause 252.204-7021) builds upon the NIST SP 800-171 DoD Assessment Methodology by adding a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level. The CMMC is designed to increase assurance to the DoD that federal contract information (FCI) and DoD Controlled Unclassified Information (CUI) is protected at a level commensurate with the risk. The CMMC requirement flows down to subcontractors.

6.5.4.1 The Contractor shall have a current (i.e., not more than three years old) CMMC certificate in SPRS issued by an accredited CMMC Third Party Assessment Organization (3PAO) at the required CMMC level. The description of CMMC levels is available at https://www.cmmcab.org/.

6.5.5 The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the CO or COR, for consideration by the DoD Chief Information Officer (CIO). The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be non-applicable or to have an alternative, but equally effective, security measure that may be implemented in its place.

6.5.6 If the DoD CIO has previously adjudicated the Contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a

DRAFT

copy of that approval shall be provided to the CO or COR when requesting its recognition under this contract.

6.5.7 Cloud Computing: If the Contractor intends to use an external cloud service provider, on their behalf, to store, process, or transmit any DoD CUI in performance of this contract, the Contractor shall require the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/) and that the cloud service provider complies with requirements in paragraphs 6.5.8 through 6.5.14 for cyber incident reporting, malicious software, media preservation and protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.

6.5.7.1 If the information is DoD CUI-specific (e.g., PII/PHI), then the Contractor shall ensure the external cloud service provider meet the security requirements equivalent to FedRAMP High baseline.

6.5.8 **Cyber Incident Reporting Requirement**

6.5.8.1 When the Contractor discovers a cyber incident that affects a covered Contractor information system or the covered defense information residing therein, or that affects the Contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall:

6.5.8.1.1 Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered Contractor information system(s) that were part of the cyber incident, as well as other IS on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support;

6.5.8.1.2 In accordance with DFARS clause 252.204-7012, rapidly report (within 72 hours) cyber incidents involving DoD CUI to DoD Cyber Crime Center (DC3) via https://dibnet.dod.mil/portal/intranet/. In the event of a cybersecurity incident involving a CUI-Specific breach (i.e., PII/PHI), the Contractor, in addition to reporting to the DC3, shall follow the incident reporting guidance prescribed in the TRICARE Operations Manual, Chapter 1, Section 5, "Compliance with Federal Statutes" at https://manuals.health.mil/

6.5.8.2 Cyber incident report: The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements as prescribed at the https://dibnet.dod.mil/portal/intranet/.

DRAFT

6.5.8.3 Medium assurance certificate requirement: In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/

6.5.9 Malicious software: When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DC3 in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

6.5.10 Media preservation and protection: When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected IS and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

6.5.11 Access to additional information or equipment necessary for forensic analysis: Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

6.5.12 Cyber incident damage assessment activities: If the DoD elects to conduct a damage assessment, the CO will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of DFARS clause 252.204-7012.

6.5.13 Apply other IS security measures when the Contractor reasonably determines that IS security measures may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., HIPAA) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.

6.5.14 The Contractor shall maintain within the US or US territories all Government data that is not physically located on DoD premises, unless the Contractor receives written notification from the CO to use another location, in accordance with DFARS 239.7602-2(a).

6.5.15. 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).

6.6 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)

DRAFT

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.

DRAFT

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-

DRAFT

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.

DRAFT

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

DRAFT

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:

DRAFT

(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.

DRAFT

(b) For DBB and DB MILCON-funded FRCS, the Contractor proceeds at its 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's 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

DRAFT

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.

DRAFT

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.

DRAFT

6.7.9.3 The Contractor shall maintain continually monitor the authorized security configuration and notify the government within forty-eight (48) 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) 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.

DRAFT

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.

DRAFT

6.11 **System Authorization Acess 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. 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.

DRAFT

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**

DRAFT

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.

PART 7, ATTACHMENT 1 PERFORMANCE REQUIREMENTS SUMMARY

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)	Method of Surveillance

DRAFT

Performance Requirements Summary (PRS) # 1. The Contractor shall deliver a fully functional and integrated ESS for NHB, which is compliant with the applicable publications in Section 2.3 of this PWS	5.1.1	100%	Random inspection

DRAFT

7.2 Other Attachments

Attachment 2, Deliverable Schedule Table (Paragraph 6.5.2.1.1)

Attachment
2-Deliverable Schedul

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

DRAFT

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 task order award	Contractor's format	CO	All, See PWS 1.10.1
CDRL A002 – Training Plan and Materials	30 days prior to the training	Contractor's format	COR	PWS 5.7.3
CDRL A003 – Final "As-Built" Drawings, User Manuals, and Maintenance Procedures	Upon system acceptance	Contractor's format	COR	PWS 5.7.4

DRAFT