Department of Defense
Defense Health Agency
Performance Work Statement

DEFENSE HEALTH AGENCY ENTERPRISE (OFF-SITE) TELERADIOLOGY SERVICES

Solicitation Number: TBD
Version: DRAFT 0.1
Date: 7 JULY 2026

PART 1
1.0 GENERAL INFORMATION

1.1 Background: The Defense Health Agency (DHA) is a joint, integrated Combat Support Agency that enables the Army, Navy, and Air Force medical services to provide a medically ready force and ready medical force to Combatant Commands in both peacetime and wartime. The DHA uses the principles of Ready Reliable Care to advance high reliability practices across the Military Health System by improving our system operations, driving innovative solutions, and cultivating a culture of safety.

1.2 Objective: Provide a standardized enterprise teleradiology services contract for DHA MTFs to employ to optimize radiology capabilities, especially for on-call support and overflow work.

1.3 Scope:
1.4.1. This is a **non-personal services contract** for credentialed and privileged professional diagnostic radiology services. Services shall be performed at Contractor facilities by board certified radiologists in support of basic assistance with case volume and on-call scenarios throughout the Military Health System (MHS). The supported DHA MTFs include medical centers, hospitals, clinics, and similar facilities located worldwide, both within the continental United States (CONUS), outside the continental United States (OCONUS), and in U.S. Territories. All patient age groups are covered.

1.4.2. Services shall be performed using Department of War (DoW) approved secure broadband connections as indicated herein to transmit radiology images and data between the requiring DHA MTFs and the Contractor's facilities.

1.5 Description of services: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform professional diagnostic radiological services as defined in this Performance Work Statement (PWS) except for those items specified as government furnished property and services.

1.5.1 Teleradiology services shall include professional preliminary and final interpretation, as well as specific consultation as needed. The services provided in this contract will be utilized to supplement DHA MTF radiologists, including any terms and conditions defined in Task Orders (TOs) issued under this contract. Examinations include Radiography, Ultrasound, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), nuclear medicine, bone densitometry, dental cone beam CT, and PET/CT.

1.5.2 The Contractor shall provide complete and accurate diagnostic interpretations of radiology examinations performed by Government personnel and provide further professional consultation that relates to diagnostic imaging, upon request, to members of the medical staff.

1.5.2.1.“Examinations" as referred to herein consists of individual patient diagnostic imaging examinations.

1.5.2.2. “Interpretations” may include preliminary and final interpretation of one or more images from examinations. Further professional telephone consultation may be required upon request of the user.

1.5.3. The Contractor must be authorized to connect to and transmit data between the Army, Navy, Air Force, and DHA Medical Community of Interest (MEDCOI) Information Networks and have computer hardware that is capable of receiving Digital Imaging and Communications in Medicine (DICOM) compliant diagnostic imaging studies from the requiring MTF and to return a final interpretation report that will automatically upload into the patient’s Electronic Health Record (EHR).

1.6 Period of Performance (PoP): The PoP shall be specified in the base enterprise teleradiology contract. Each task order PoP shall be coterminous with the base PoP.

1.6.1 Transition Period: A 180-calendar-day base contract transition period will commence prior to commencement of the ordering period,. Task orders will provide at least 30 calendar days between task order award and start of performance, but task order transition periods will not be invoiceable.

1.6.1.2. Requirements During Transition Periods

1.6.1.2.1. The Contractor shall have a project manager available during all transition periods to complete requirements listed in part 4 of this PWS.

1.6.1.2.2. The transition-out period occurs 60 calendar days prior to the end of the final period of performance of this contract and will include turnover/closeout/purge of any residual Government data and general cooperation with the successor Contractor. If the Contracting Officer (KO) requires additional transition efforts by the incumbent in transitioning a successor Contractor, FAR Clause 52.237-3 Continuity of Service may be invoked and associated costs will be negotiated in accordance with the terms of this clause at that time.

1.7. Place of performance: The work shall be performed at Contractor facilities inside the United States.

1.8 Standards: Contractor shall comply with all applicable federal, state, and local laws, DoW, DHA, agency-specific, installation, and MTF policies, procedures, and instructions.

1.9 Recognized Federal holidays: services may be required on federally recognized holidays as outlined in the TO. Recognized federal holiday:

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

1.10. Hours of operation: The Contractor shall provide services seven days per week, twenty-four (24) hours per day, and on federal holidays.

1.13 Conduct: Contractor personnel shall adhere to standards of conduct as established by the policy letters of the DHA Director, and other applicable Department of War policies.

1.14 Post Award Conference The Contractor shall attend a virtual post-award conference.

1.15 Quality

1.10.1 Quality Control (QC): The contractor shall develop and maintain an effective quality control 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 quality control program is the means by which the work complies with stated requirements. The QCP is to be delivered within 10 days after date of award. A comprehensive written QCP shall be submitted to the KO and COR within 5 working days when changes are made thereafter. After acceptance of the Quality Control Plan Quality Control Plan (QCP) the contractor shall receive the KO's acceptance in writing of any proposed change to his QC system.

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).

1.16 Contractor personnel

1.11.1 CAC requirements: All contract radiologists must have an EDIPI as required by MHS GENESIS for studies to be accepted. A CAC is not required.

1.11.2 Contractor onboarding and training. The contractor shall complete all requirements, training, and forms per the following DHA instructions:

1.11.2.1 The DHA's 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. This document will be provided to the Contractor as required.

1.11.2.2 The DHA's Contractor training instructions embedded at Part 7 Section 7.6.

1.11.3. Contractor Radiologists: Radiologists assigned by the Contractor to provide the official interpretation of images transmitted by teleradiology must maintain licensure appropriate and necessary to deliver services. Physicians providing services under this contract must be privileged by the guidelines set by accrediting organization and IAW DHA guidelines prior to execution of service. Credentials and privileges must be current/maintained while providing service. The first time the Contractor provides services to each MTF during TO execution under this contract, the Contractor will provide that MTF credentials office a list of all radiologists (Provider Listing), by name and NPI that the Contractor intends to utilize for services. That MTF will inform the Contractor when radiologists are authorized to provide services after a verification process. The Contractor will notify each MTF receiving services when radiologists already providing services or planned to provide services to that MTF change within 24 hours of the change. The Contractor will submit a semi-annual Provider Activity Report (every 6 months) of practice activity to the Privileging Authority MTF that includes number and type of examinations reported under this contract with reporting radiologist name and NPI grouped by Originating Site MTF. The Contractor shall ensure professional liability coverage is always maintained in accordance with jurisdictional requirement of each state in which services are being performed. Proof of coverage shall be provided to the enterprise level COR.

1.11.3.1 Qualifications and Requirements: Contract radiologists performing services under this PWS shall possess the skills, knowledge and abilities to perform such services. The Contractor shall meet the following requirements for education and training, certification, experience, licensure, credentialing/privileging, and continuing medical education.

1.11.3.2 Education and Training: The Contract radiologists shall hold the degree of either a Doctor of Medicine (MD), Doctor of Osteopathy/Osteopathic Medicine (DO), or have completed the Educational Commission for Foreign Medical Graduates certification process, be eligible for medical licensure in the United States, and shall have successfully completed an approved residency program in diagnostic radiology.

1.11.3.3 Board Certification(s): Each contract radiologist shall hold and maintain a current certification from the American Board of Radiology or the American Osteopathic Board of Radiology in diagnostic radiology and shall otherwise comply with all applicable Joint Commission and American Hospital Association standards. The National Institute for Occupational Safety and Health (NIOSH) shall certify each contractor performing B-Reads. The NIOSH certification demonstrates proficiency in classifying radiographs of pneumoconiosis according to the International Labour Office (ILO) standardized classification system.

1.11.3.4 The Contractor shall provide radiologists capable of interpreting studies on patients of all ages.

1.11.3.5 A Contractor performing teleradiology services shall understand the basic technology of image acquisition, transmission, manipulation, processing, archiving, retrieval, and display, including the strengths, weaknesses, and limitations of different methods. They shall be knowledgeable in how to optimally utilize the image viewing equipment. The Contractor

performing the official interpretation shall be responsible for the quality of the images being reviewed and understand the elements of Quality Control (QC) of digital image management systems. The Contractor shall demonstrate qualifications in accordance with the appropriate ACR Practice Guideline or Technical Standard for the particular diagnostic modality being interpreted.

1.11.3.6 Experience: The contract radiologists shall have been continuously employed in the practice of diagnostic radiology or in clinical radiology training for 24 months within the last 36 months. Time spent in an administrative capacity as a claims reviewer, medical school instructor, medical director, etc. does not qualify as practicing time.

1.11.3.7 Licensure: The Contractor shall have and maintain a current, active, valid, and unrestricted license to practice medicine in the State (to include D.C. or US Territory, where the images originate as well as the State or US Territory where interpreted). If images originate outside the US or US Territories, only a current, active, valid, and unrestricted State license in the State in which the images are interpreted is required. In the event a radiologist changes his/her interpretation location, that radiologist shall not interpret examinations until a license is obtained from the new location and the license is presented to the credentialing office of the MTF affected (this applies if the radiologist is not already in possession of that location's license). The Contractor shall not use any radiologists licensed only by a foreign country or are physically located in a foreign country.

1.11.3.8 Credentialing/Privileging: The Contractor shall ensure each radiologist obtains clinical privileges from the MTF Privileging Authority prior to beginning work. The Contractor shall follow the clinical privileging processes and requirements outlined in the PWS and each TO (if applicable). Contractor shall plan for up to 60 calendar days for Government review and approval with granting of privileges. The clinical privileges granted by the MTF will be sufficient to allow for performance of all specific tasks identified in this contract. If a radiologist is not privileged to perform all the specific tasks in this contract, the radiologist will not be allowed to provide services under this contract, and the Contractor shall provide another radiologist. The Contractor shall ensure that each radiologist remains privileged.

1.11.3.8.1 The Contractor shall ensure successful completion of the credentialing and privileging process by the Privileging Authority MTF for all contract radiologists and that each Originating Site MTF acknowledges all contract radiologists designated by the Contractor to provide services for that MTF are authorized prior to providing services.

1.11.3.8.2 The Contractor shall, on a continuing basis, verify all information submitted to the MTF for the purpose of credentialing/privileging. During the term of the contract, the Contractor shall notify the privileging authority MTF and any affected Originating Site MTFs upon becoming aware of any information that may compromise the radiologist's privileges at the MTF within 24 hours. This includes, but is not limited to, information linking the radiologist with chemical dependency, a requirement or change in licensure status, a felony or malpractice. The information will be reviewed and may result in rescinding privileges.

1.11.3.8.3. Once privileges are granted, subsequent actions taken concerning the privileges of radiologists, including any limitation on privileges, will be governed by the procedures described in DHA PM 6025.13, this PWS, and each TO (if applicable). Action that suspends, revokes, or otherwise restricts the privileges of a radiologist results in that radiologist not being authorized to perform under the contract. Such action does not excuse the Contractor from providing

performance. Any lapse in coverage may be considered as cause for grounds for termination of the contract, at the discretion of the KO. Requirements for privileging or for licensing verification are the same for replacement radiologists.

1.11.3.8.4 The MTF Privileging Authority is the sole authority who can revoke or otherwise restrict the privileges of any radiologist who he/she determines is not qualified to perform the contract services. Adverse actions on radiologist privileges, once the Commander/Director takes action, may be appealed in accordance with DHA PM 6025.13, Vol 3, but may not be appealed by the Contractor. All documents generated through professional review activities are protected as Medical Quality Assurance Program (MQAP) documents, in accordance with Section 1102 of USC Title 10.

1.11.4 Radiologists who have previously undergone MTF adverse action processes resulting in an adverse action outcome (e.g., privilege revocation or restriction) or have otherwise been determined by the Government to be ineligible to perform contracted services are excluded from providing services under this contract. The current CQM process/reviews for non-personal services contractors' process is in DHA-PM 6025.13:

1.11.5 Continuing Health Education (CHE)/ Certified Education Units (CEU) Requirements: Contractor personnel registered or certified by national/medical associations shall continue to meet the minimum standards for CHE to remain current as prescribed by the State licensure and maintenance of board certification requirements. The Government will not reimburse for these costs.

1.17 U.S. Citizenship

Radiologists performing under this contract must be U.S. citizens. The Government shall not be held liable for not allowing performance under this contract by a contractor employee who fails to comply with, or to maintain, the citizenship or legal alien status requirements stated herein.

1.18 English language requirement: The Contractor shall ensure that all Contractor personnel providing services under this contract are able to read, write, and speak English fluently.

1.19. Continuity of service**s**: The Contractor shall ensure sufficient staffing and resources to provide all required services and support throughout the term of the contract.

1.19.1. The Contractor shall provide a point of contact that is available via telephone 7 days a week, 24-hours per day, Monday through Sunday, including Federal Holidays.

1.19.2. The Contractor shall notify the KO and no later than five calendar days prior to change of any management personnel or other personnel that represent the contract to the government. The notification shall be submitted in writing,

1.20. Conflict of interest: The Contractor shall not employ any person who is an employee of the United States Government if the employment of that person would create a conflict of interest. The Contractor shall not employ any person who is an employee of the Department of Defense, either military or civilian, unless such person seeks and receives approval IAW DoD Directive (DoDD) 5500.7, Standards of Conduct, 29 Nov 07, and Service policies, and the contracting officer provides prior contract approval.

1.21. Invoicing and billing: The Government will only pay for services ordered. If the Contractor submits invoices for services that were not ordered by the government, it may constitute fraud or a false claim and may result in administrative or criminal action or both.

1.21.1 Billing of beneficiaries. The Contractor shall not bill the patient for services rendered under this contract. The Contractor shall not accept compensation of any kind for patients treated, procedures performed, or any other actions performed, except under the terms and conditions of this contract, at the rate specified in the bid schedule.

1.18.2. Some exams consist of images that could be considered as more than one study. However, these examinations shall only be billed as one study when there exists a single Current Procedural Terminology (CPT) code that describes the examination. Examples of such examinations include CT Abdomen/Pelvis, CT or MRI with and without contrast of same body region, bilateral hip x-ray and bilateral rib x-ray. See Appendix B, paragraph 1: "Requirements for counting of examinations for CLIN charges described by modality" for additional description of these requirements.

1.22 Non personal services**:** This is a non-personal services agreement. Contractor personnel are subject to neither the supervision nor control of a government officer or employee. The Contractor personnel shall perform their duties IAW specific tasks outlined in this PWS/resultant contract and TOs (if applicable). Supervisory functions and managing Contractor employees, such as hiring, directing, counseling, and firing of Contractor personnel are the responsibility of the Contractor and performed by the Contractor, not the Government.

1.20 Communication**:** The Contractor shall ensure contract providers maintain open and professional communication with providers in the MTF. The Contractor shall abide by federal and local MTF regulations and requirements concerning the confidentiality of patient records, as embodied in federal statutes including the Privacy Act of 1974 and the Health Insurance Portability & Accountability Act (HIPAA) of 1996. All medical records and reports will remain the property of the Government.

1.21 PII/PHI, and federal information requirements: See Appendix F of this PWS.

1.22 Privacy act program**: The** Contractor shall create, maintain, and destroy Privacy Act data IAW 38, USC 5701, and 38 USC 7332; and Privacy Act systems of records notice(s) (http://dpcld.defense.gov/Privacy /SORNs.aspx). If the Contractor receives a Privacy Act request, the Contractor shall be responsible for searching for the records and providing those records to a Government official who, as the authorized official, will make the decision on releasing the Government records.

1.23 HIPAA and Privacy Act Training**:** Contractor personnel requiring network access to the hosted applications shall successfully complete the MHS Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security training prior to access to the hosted applications and then annually thereafter. The Contractor shall submit a copy of the Privacy Act and HIPAA course certificate along with the completed System Authorization Access Request (SAAR) and DoD IA Awareness training certificate to the TO level COR for each affected Contractor personnel. The Contractor is responsible for maintaining an active database of Contractor employee HIPAA and Privacy Act training status and providing initial and annual training certificates to the TO COR, as requested. The course is accessible via Joint Knowledge Online (JKO). Please refer to the Joint Knowledge Online (JKO) Instructions on accessing JKO.

1.28. Functional requests**:** A functional request is a written request for DOD records received from any person (including a member of the public), or a business that does not cite either the FOIA or Privacy Act. The Contractor shall direct requests to the COR and KO.

1.29. Release of Medical Information: The provider shall only release medical information obtained during the course of this contract to other MTF staff involved in the care and treatment of that individual patient. All patient information will comply with HIPAA standards included in Appendix F of this PWS.

1.30. Indemnification and Medical Liability Insurance: The Contractor shall provide and maintain adequate liability coverage for their employees, consistent with the risks associated with the performance of all services required by this PWS/contract. Refer to Federal Acquisition Regulation (FAR) clause 52.237-7, "Indemnification and Medical Liability Insurance." If the Contractor uses subcontractors in the performance of this contract, the Contractor is required to ensure that its subcontracts for provisions of healthcare services contain the requirements of FAR clause 52.237-7, including the maintenance of medical liability insurance.

1.31. The Contractor shall be responsible for any liability producing acts or omissions arising from its radiologists' performance. The Contractor shall indemnify the Government against all claims by third parties for death or bodily injury (including sickness or disease) to the extent that such a claim arises in any way from Contractor performance under this contract. In the event of litigation/investigation of a claim or malpractice, the Contractor shall ensure its radiologists' full cooperation with Government authorities and designated officials in investigation of claim and/or preparation of litigation.

1.32. If any suit or action is filed or any claim is made against a contract radiologist resulting from work performed by the contract radiologist under this contract, the contract radiologist shall immediately notify the privileging authorities and the Contractor, who in turn shall notify the COR and KO. The Contractor shall promptly furnish copies of all pertinent papers received.

1.33. Inquiries, Comments, or Complaints. All inquiries from the media, third parties, private or public agencies shall be relayed within 24 hours to the COR and TOKO or KO, as applicable. The Contractor shall not respond directly to these or any inquiries. All inquiries, comments or complaints arising from any matter observed, experienced, or learned of as a result of or in connection with the performance of this contract, the resolution of which may require the dissemination of official information, shall be directed to the

Contracting Officer Representative (COR) and TOKO or KO, as applicable.

1.34. Patient lists. All patient lists, no matter how developed, shall be treated as privileged information. Lists and/or names of patients shall not be disclosed to or revealed in any way to any unauthorized person or for any use outside the MTF without prior written permission by the MTF Commander/Director, in accordance with federal law, to include the Privacy Act, the Health Insurance Portability and Accountability Act (HIPAA) (see Appendix F) and DHA and Service specific requirements denoted in each contract and TO.

1.35 Physical security: The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use.

1.38 Contractor Program manager: The Contractor shall provide skilled, experienced professional and/or technical personnel essential for successful Contractor accomplishment of the work to be performed, otherwise defined as "program manager". The Contractor shall

designate and electronically submit to the KO, program manager contact information, to include phone and email, at least five business days prior to contract performance start date.

1.38.1 Qualifications for the program manager a: The Program Manager shall possess 5 years' experience. 1.38.2 Program Manager The designated program manager shall communicate with the contract COR(s), via phone or email, at a minimum, monthly and when requested by the COR to discuss any problems the Contractor may be experiencing during the performance of this contract. Program manager shall be available via phone and email in the event of emergencies to include weekdays, weekends, and holidays. The program manager or alternate shall be available between 9:00 a.m. to 5:30p.m. ET, Monday through Friday except Federal holidays or when the government facility is closed for administrative reasons. If program manager is unavailable for work under this contract for a continuous period exceeding thirty (30) business days, the Contractor shall immediately notify the KO in writing and promptly replace such program manager with personnel of at least substantially equal ability and qualifications.

1.38.2 Designated program manager shall be available to discuss all aspects of performance during the life of the contract and have the authority to resolve issues and problems as they arise. The designated program manager shall have full authority to act on behalf of the Contractor on all contractual matters relating to contract.

1.39 Data rights: The Government will maintain data rights to all documents/material produced under this contract. All documents and materials produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/ copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the Contractor without written permission from the KO. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.40 Reporting

1.40.1 Reserved.

1.40.3 Government's COR: The Government will identify a COR for the contract and for each TO. 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,; monitor Contractor's performance and notifies both the KO 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.

1.40.4 Periodic Performance meetings: The Contractor Program Manager is required to attend contract level and task order performance meetings when requested by the Government. Required attendance is virtual. . The time and location will be identified upon the issuance of the award. All key Contractor and Government representatives shall attend either in person or

virtually. . These meetings shall be at no additional cost to the government. Task orders may include additional requirements for these meetings.

1.41 Contractor Identification

1.41.1 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 understand 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 understand that the person is contractor support personnel.

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

1.41.3 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.

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

1.42.1 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 Facilities Security Officer/Security POC shall submit a Standard Form (SF) 85/86 to DHA's Personnel Security Office for a background investigation.

1.42.2 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.

1.43. Personnel Security

1.43.1 The contractor shall comply with DoD 8570.01-M, “Information Assurance Workforce Improvement Program,” December 19, 2005 as amended; DoDI 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”, 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),” dated April 3, 2017 as amended. Contractor responsibilities for ensuring personnel security include, but are not limited to, meeting the following requirements:

1.43.1.1 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) 681-6777.

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

1.43.1.3 DHA Personnel Security Office will deny any access to any automated information system (AIS), network, or CUI if a contractor receives an unfavorable adjudication, or if information that would result in an unfavorable adjudication becomes available.

1.44. ACCESS AND GENERAL PROTECTION SECURITY POLICY AND PROCEDURES. If required to enter a Government facility, the Contractor, to include associated subcontractor employees, shall comply with applicable installation, facility, and area commander installation/facility access and local security policies and procedures (provided by Government representative). The Contractor shall also provide all information required for background checks to meet installation access requirements to be accomplished by installation Provost Marshall Office, Director of Emergency Services or Security Office. The Contractor shall comply with all personal identity verification requirements as direct by DoD, Services, and or local policy. In addition to the changes otherwise authorized by the changes clause of this contract, should the Force Protection Condition (FPCON) at any individual facility or installation change, the Government may require changes in Contractor security matters or processes.

1.441. Contractor shall complete required security background checks and obtain the minimum required clearance prior to starting work.

1.44.2. It is the Contractor's responsibility to ensure its employees undergo proper criminal history background checks by providing the Government support, cooperation and active assistance throughout the process.

1.44.3. All Contractors requiring access to their systems for administrative/maintenance support of systems/applications on the DoD network will meet DoD requirements for a privileged-level account before being granted a network account. Position of Trust is the minimum eligibility for Information Assurance Technical level II (IAT-II) which is required for B2B Gateway/DoD network access. Contractors designated as filling IAT II positions shall be responsible for obtaining and maintaining a Tier 3 (T3) investigation. It is the Contractor's responsibility to ensure security background investigations are completed prior to starting performance on the contract. This includes following the DoD Access Process attached in Section 7.1, and Attachment D of this PWS, submitting all required paperwork, and submitting fingerprints to the appropriate DHA security office. A favorable Tier 3 (T3) investigation is required to perform IAT-II duties.

1.44.4. The preferred method for the submission of fingerprints is via digital fingerprint machine through the Defense Manpower Data Center (DMDC) Secure Web Fingerprint Transaction (SWFT +) System. Digital fingerprints may be submitted at designated Government facilities, using the SOI and SON obtained by the DHA security office. If digital fingerprints are not possible, a candidate must submit ink prints on the Standard Form 87 Fingerprint Card. The use of hard copy fingerprint cards will delay the security review. The preparation and submission of the Tier 3 shall be at the expense of the Contractor, upon commencement of services. The

Contractor shall advise their employees that a Government approved background check is needed as a condition of employment under this contract.

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

2.1 Definitions.

American College of Radiology (ACR). The principal nonprofit, professional organization of radiologists, radiation oncologists, and clinical medical physicists in the United States

B-Read. A more sophisticated interpretation of the chest x-ray that may identify exposure and illness caused by substances such as silica and asbestos.

Beneficiary. An individual eligible and entitled to military healthcare system (MHS) benefits under provisions of Title 10 U.S.C. Chapter 55, which generally include Active Duty, Service members, retirees, certain reserve and national guard members, and eligible dependents and survivors.

Business-to-Business (B2B) Gateway. B2B gateways enable information exchange from one business partner to another. B2B gateways provide e-commerce platforms via a centralized point for transformation of multiple data sources using established interoperability standards.

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

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

Certification. An official recognition by a national agency or association that the individual worker has successfully completed an approved education program or evaluation process. This includes formal processes designed to assess the knowledge, experience, skills and abilities required to provide quality services.

Clinical Privileges. The permission to provide medical and other patient care services in the granting organization, within well-defined limits, based on the individual's education, professional license, training, experience, current competence, judgment and health.

Clinical Privileging. The granting of permission and responsibility of a healthcare provider to independently provide specified or delineated healthcare within the scope of his or her license, certification, or registration. Clinical privileges define the scope and limits of practice for individual providers and are based on capability of the healthcare facility, licensure, relevant training and experience, current competence, health status, judgment, and peer and department head recommendations.

Clinical Quality Management. A collection of programs that emphasize leadership, commitment to quality performance, regardless of the practice site, a supportive organizational culture, and evaluation of the effectiveness of clinical performance improvement activities.

Commander/Commanding Officer. The individual (military officer) responsible for the operations of the MTF for which the contract services are provided.

Competence. The state of having adequate ability and up-to-date knowledge to perform the duties, functions, and requirements of a particular discipline, job or duty position in accordance with credentialing requirements.

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

Contract Service Provider. For the purpose of this contract, "contract service provider" means an individual employed by the prime or subcontractor. Also see "Health Care Provider."

Contractor. The entity or its representative responsible for the delivery of the services or materials specified in the contract, as designated by contract award.

Credentialing. The process of obtaining, verifying, and assessing the qualifications of both privileged and non-privileged providers to provide safe patient care services. This assessment serves as the basis for decisions regarding delineation of clinical privileges, as well as appointments and reappointments to the medical staff. The required information should include qualification data such as relevant education, training, and experience; current licensure; and specialty certification (if applicable) as well as performance data, such as current competency, and the ability to perform the selected privileges. This data is collected, verified, and assessed initially and on an ongoing basis.

Cyber Incident. Actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein. (DoDI 8582.01, December 2019)

Defense Health Agency (DHA). Defense Health Agency (DHA) is a combat support agency that provides a host of shared health services across the MHS, from operating the TRICARE health benefit to providing pharmacy and medical logistics, performing medical research and development and operating health information technology systems, with a goal of providing integrated and efficient service to the joint force.

Digital Imaging and Communications in Medicine (DICOM). A standard for interconnection of medical digital imaging devices, developed, and sponsored by the American College of Radiology and the National Electrical Manufacturers Association, consisting of a standard image format and a standard communications protocol.

Digital Imaging Network Picture Archiving and Communications Systems (DINPACS or PACS). A medical imaging system used for storing, retrieving, presenting and sharing images produced by various medical hardware modalities, such as X-ray, CT scan, MRI and ultrasound machines.

Digital Radiography. A digital radiography detector (active) used to describe a flat-panel digital x-ray system that reads the transmitted x-ray signal immediately after exposure with the detector in place.

Distant Site (or receiving site). The location of the Contractor providing teleradiology services. See also "originating site" below.

Healthcare Information and the Management Systems Society (HIMSS). A professional non-profit healthcare organization dedicated to improving health care in quality, safety, cost-effectiveness, and access through the best use of informational technology and management systems.

Health Layer Seven (HL7). A set of international, standardized protocols and clinical messaging formats designed to facilitate the transfer, integration, sharing, and retrieval of electronic health information across diverse healthcare systems. DHA utilizes Corepoint Rhapsody to proctor HL7 information between MHS GENESIS and any system requiring HL7.

License. A grant of permission by an official agency of a State, the District of Columbia, or a Commonwealth, territory, or possession of the United States to provide healthcare within the scope of practice of a specified discipline. Licenses must be:

- Current: Active, not revoked, suspended, or lapsed in registration.
- Active: Characterized by present activity, participation, practice, or use.
- Valid: The issuing authority accepts, investigates, and acts upon quality assurance information, such as practitioner professional performance, conduct, and ethics of practice, regardless of the practitioner's military status or residency.
- Unrestricted: Not subject to limitations on the scope of practice ordinarily granted all other applicants for similar specialty in the granting jurisdiction.
- Providers in the MHS may not have one active license and another currently suspended or probationary license. For example, if a provider is licensed in both Texas and Tennessee, and the provider's Texas license is active, but the provider's Tennessee license is on probation, restricted, or is temporarily suspended, the provider would not meet requirements for clinical practice in the MHS.

Military Health System (MHS). Enterprise within the United States Department of Defense that provides health care to active duty and retired U.S. Military personnel and their dependents.

MHS GENESIS. MHS GENESIS, the new electronic health record for the Military Health System, provides enhanced, secure technology to manage health information. This system is based on Cerner millennium, and its RadNet module is the new new MHS Radiology

Information System, which generates radiology order messages and receives radiology report messages.

Military Treatment Facility (MTF). A medical center, military hospital or clinic to include dental and veterinary clinics. The MTF includes all activities providing outpatient and/or inpatient health care services for eligible beneficiaries. Originating site (or transmitting site). The location of the MTF where the patient obtained the radiological images. See also "distant site" above.

Non-DoD Information System. Any information system that is not owned, controlled, or operated by the DoD and that is not used or operated by a contractor or other non-DoD entity exclusively on behalf of the DoD. Includes information systems owned and operated by other departments and agencies of the U.S. Government; State and local government; allies, coalition members, host nations and other nations; multinational organizations; non-government organizations; and the private sector. (Reference: DoDI 8582.01, December 9, 2019)

Non-Personal 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.

Non-Routine Communication. Reference ACR Practice Parameter for Communication of Diagnostic Imaging Findings Revised 2014 (Resolution 11)

Originating Site. The site where the patient is physically located and medical imaging is acquired.

Picture Archiving and Communication System (PACS). See DINPACS.
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.

Privileging Process. The process established by the MTF for granting clinical privileges to Radiologists.

Protocol. Applies to information technology; a set of guidelines by which two different computer devices communicate with each other.

Radiography. A digital radiography detector (passive) system that uses a storage phosphor plate contained in a cassette instead of a film-screen cassette. A laser beam scans the exposed plate to produce the digital data that is then converted into an image.

Quality Assurance. Actions taken by the Government to assess services to determine if performance meets the requirements of the contract.

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 quality assurance surveillance plan or require the offerors to submit a proposed quality assurance surveillance plan for the Government's consideration in development of the Government's plan.

Quality Control. Actions taken by a Contractor to control the performance of services to ensure performance meets the requirements of the contract.

Radiologist. (Or, collectively, "Radiologists") shall mean individual physicians employed by the Contractor to perform duties pursuant to this contract who shall possess the qualifications specified herein. (Alternative phrasing: "Health Care Provider.")

Society for Imaging Informatics in Medicine (SIIM). A healthcare professional organization representing the interests and goals of those who work with and are affected by the rapidly changing world of imaging technologies and information management.

Special Finding. Any abnormal, life threatening, or significant findings.

STAT. At once/immediately, as commonly used in medical terminology for the Latin "statim." Check Section 5 for ensuring ordering Contractor provides phone number.

Technical Standard. For the purpose of a technical standard, the images referred to are those that Contractor's diagnostic radiologists would normally interpret, including transmission projection and cross-sectional X-ray images, ionizing radiation emission images, and images from ultrasound and magnetic resonance modalities. Research, non-human and visible light images (such as dermatologic, histopathologic, or endoscopic images) are out of scope and not applicable to this effort.

The Joint Commission (TJC). A national organization dedicated to improving the care, safety, and treatment of patients in healthcare facilities; publishers of the Joint Commission Accreditation Manual for Hospitals and the Ambulatory Healthcare Standards Manual.

Teleradiology. The transmission of radiological patient images, such as radiographs, Computed Tomography (CT) and Magnetic Resonance Imaging (MRI), from one location to another for the purposes of remote study interpretation.

2.2 Acronyms and Abbreviations

ACO Administrative Contracting Officer
ACR American College of Radiology
ADP/IT Automated Data Processing/Information Technology
AHLTA Armed Forces Health Longitudinal Technology Application
AIS Automated Information System
AKO Army Knowledge Online

AQL Acceptable Quality Level
AR Army Regulation
ARRT Acquisition Requirements Roadmap Tool
ATCTS Army Training Certification Tracking System
ATO Authority to Operate
AVHE Application Virtualization Hosting Environment
B2B Business-to-Business
BBP Best Business Practices
CAC Common Access Card
CAP Cloud Access Point
CDI Covered Defense Information
CDRL Contract Data Requirement List
CE Computing Environment
CFR Code of Federal Regulations
CHCS Composite Health Care System
CIO Chief Information Officer
CJCSM Chairman of the Joint Chiefs of Staff Manual
CLIN Contract Line Item
CME Continuing Medical Education
CMR Contractor Manpower Reporting
CNSSI Committee on National Security Systems Instruction
KO Contracting Officer(s)
CONUS Continental United States (excludes Alaska and Hawaii)
COR Contracting Officer’s Representative
COTR Contracting Officer's Technical Representative
CR Computed Radiography
CSP Cloud Service Provider
CSP Contract Service Provider
CSSP Cyber Security Service Provider
CT Computed Tomography
CUI Controlled Unclassified Information
CV Curriculum Vitae
DA Department of the Army
DACA Days after contract award
DAD-A Deputy Assistant Director for Acquisition
DC3 DoD Cyber Crime Center
DD 254 Department of Defense Contract Security Requirement List (if applicable)
DFARS Defense Federal Acquisition Regulation Supplement
DHA Defense Health Agency
DICOM Digital Imaging Communication Medicine
DINPACS Digital Imaging Network Picture Archiving and Communications Systems
DISA Defense Information System Agency
DO Doctor of Osteopathy/Osteopathic Medicine
DoD Department of Defense
DODD Department of Defense Directive
DODI Department of Defense Instruction

DoDM Department of Defense Manual
DR Digital Radiography
EHR Electronic Health Record
EULA End User License Agreement
EVM Earned Value Management
FAR Federal Acquisition Regulation
FedRAMP Federal Risk Authorization and Management Program
FIPS Federal Information Processing Standard
FISMA Federal Information Security Management Act
FSO Facilities Security Officer
FY Fiscal Year
HA Health Affairs
HCA Head of the Contracting Activity
HCP Health Care Provider
HIMSS Healthcare Information and Management Systems Society
HIPAA Health Insurance Portability and Accountability Act
HIT Health Information Technology
HL7 – Health Layer Seven
I/O In/Out Processing Portal
IA Information Assurance
IAW In accordance with
IGCE Independent Government Cost Estimate
IS Information System
ISCM Information Security Continuous Monitoring
IT Information Technology
JTR Joint Travel Regulation
KO Contracting Officer
MD Doctor of Medicine
MEDCOM U.S. Army Medical Command
MHS Military Health System
MRI Magnetic Resonance Imaging
MTF Military Treatment Facility
NCR National Capitol Region
NDA Non-Disclosure Agreement
NIST National Institute of Standards and Technology
NLT No later than
OCONUS Outside Continental United States (includes Alaska and Hawaii)
ODC Other Direct Costs
OPSEC Operational Security
OSD Office of the Secretary of Defense
OTSG Office of the Surgeon General
P&R Personnel and Readiness
PACS Picture Archiving and Communication System
Pam Pamphlet
P-ATO Personal Authorization to Operate
PGI Procedures, Guidance and Information

PHI Protected Health Information
PII Personally Identifiable Information
PIT Platform Information Technology
PK Public Key
PKI Public Key Infrastructure
PL Public Law
POC Point of Contact
PoP Period of Performance
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
RAPIDS Real Time Automated Personnel Identification System
RFP Request for Proposal
RFQ Request for Quotation
RMF Risk Management Framework
SA System Administrator
SF Standard Form
SHARP Sexual Harassment/Assault Response and Prevention
SI Sensitive Information
SIIM Society for Imaging Informatics in Medicine
SOP Standard Operating Procedure
SP Special Publication
SRG Security Requirements Guides
STIG Security Technical Implementation Guides
TA Trusted Agent
TASS Trusted Associate Sponsorship System
TJC The Joint Commission
TO Task Order
TOKO Task Order Contracting Officer
TOS Terms of Service
US United States
USC United States Code
VPN Virtual Private Network
XML Extensible Markup Language

2.3 **Publications**

ACR–AAPM–SIIM ACR Practice Parameter for Communication of Diagnostic Imaging Findings Revised 2014 (Resolution 11)

ACR White Paper on Teleradiology Practice: A Report from the Task Force on Teleradiology Practice.
DoD Access Process Overview New Process Draft.pdf
Technical Standard for Electronic Practice of Medical Imaging
10 USC 1089 Defense of Certain Suits Arising Out of Medical Malpractice
AR 25-2 Army Cybersecurity
PL 91-596 Occupational Safety and Health Act of 1970
PL 101-647, Sect. 231 Crime Control Act of 1990
PL 102-190, Sect. 1094 National Defense Authorization Act
PL 104-191k Health Insurance Portability and Accountability Act of 1996
DHA 6025.13 DHA Procedures Manual 29 August 2019
DHA 6025.28 DHA Procedural Instruction for Standard Processes and Procedures for Communication of Laboratory and Radiology Results
DHA 6025.48 Mandatory Use of Defense Health Agency (DHA) Enterprise (Off-Site) Teleradiology Services Contract by Military Medical Treatment Facilities
DoD 5200.2-R DoD Personnel Security Program
DOD 5500.7 R Joint Ethics Regulation (JER)
DoDI 6025.13 Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS) Oct 2, 2013
DoDI 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT)
DoDI 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems
DoDM 6025.13 Medical Quality Assurance (MQA) and Clinical Quality Management in the Military Health System (MHS)
DoDM 8570.01 Information Assurance Workforce Improvement Program
DoD 6025.18-R Department of Defense Health Information Privacy Regulation
DoD 8580.02-R DoD Health Information Security Regulation
DODD 5200.2 Personnel Security Program
DODD 5400.11 Privacy Program
DoDD 8140.01 Cyberspace Workforce Management", August 11, 2015, Incorporating Change 1, July 31, 2017.

Additional Cybersecurity Regulations and Guidance
The Contractor shall use and comply with the most recent published versions of the following references (including amendments and replacements), as well as all regulations or guidance referenced within those publications:
(a) United States Law (i) The Federal Information Security Management Act (FISMA)
(ii) The E-Government Act of 2002

(b) Office of Management and Budget (OMB)

The following publications are located at https://www.whitehouse.gov/omb/agency/default

(i) Circular A-130
(ii) Guidance M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Vendors

(c) National Institute of Standards and Technology (NIST)

The following publications are located at http://www.nist.gov/publication-portal.cfm
(i) NIST Special Publication (SP) 800-37 – Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems
(ii) NIST SP 800-39—Managing Information Security Risk: Organization, Mission and Information System View
(iii) NIST SP 800-53 – Security and Privacy Controls for Federal Information Systems and Organizations
(iv) NIST SP 800-60—Volume 1 Revision 1: Guide for Mapping Types of Information and Information Systems to Security Categories
(v) NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organization," December 2016, as amended.

(d) Federal Information Processing Standards (FIPS)

The following publications are located at http://www.nist.gov/itl/fipscurrent.cfm
(i) FIPS Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules
(ii) FIPS PUB 199 – Standards for Security Categorization of Federal Information and Information Systems
(iii) FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems
(iv) FIPS PUB 201-2, Personal Identity Verification of Federal Employees and Vendors

(e) Department of Defense (DoD)

The following publications are located at http://www.dtic.mil/whs/directives/
(i) DoD Instruction 4000.19, Support Agreements, April 25, 2013, as amended
(i) DFARS § 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”
(ii) DFARS § 252.239-7009, “Representation of Use of Cloud Computing”
(iii) DoD Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
(iv) DoD Instruction 8551.1, Ports, Protocols, and Services Management (PPSM)
(v) DoD Instruction 8580.02, Security of Individually Identifiable Health Information in DoD Health Care Programs
(vi) DoD Directive 5400.11, DoD Privacy Program, Federal Acquisition Regulation 52.24-21, Basic Safeguarding of Covered Contractor Information Systems, current edition
(vii) DoDD 5505.3E, DoD Cyber Crime Center (DC3) is the single point for receiving cyber incident reports from non-DoD entities that process, store or transmit DoD UI describe in Paragraph 3.3
(viii) DoD Instruction 5220.22 “National Industrial Security Program”

(ix) DoD 5220.22-M “Industrial Security Program Operating Manual”
(x) DoD Chief Information Officer DoD Information Technology Portfolio Repository Guidance
(xi) DFARS Subpart 239.71 “Security and Privacy for Computer Systems”
(xii) Committee on National Security Systems Instruction No. 1253 “Security Categorization and Control Selection for National Security Systems
(xiii) DoDI 8520.03 “Identity Authentication for Information Systems”
(xiv) Chairman of the Joint Chiefs of Staff Manual 6510.01B “Cyber Incident Handling Program”

PART 3
3.0 GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

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

3.1.1. The Government will allow access to the Government Radiology Information System (RIS) MHS GENESIS, and the multiple Picture Archiving and Communication Systems (PACSs) that have the ability to transmit DICOM images directly from the PACS and the modalities.

3.1.2 The Government is currently using Corepoint Rhapsody HL7 which the Contractor shall utilize for directing final reports directly into the RIS at no cost to the Government.

3.1.3. The Government permits the Contractor to place an approved DICOM send station behind the Government's firewall in order to facilitate a central point of DICOM transfer once an ATO is issued.

3.1.4. Any training as required by this PWS will be described in each TO. For all training requirements, the Contractor shall coordinate with the COR for the latest access information (i.e. Government training sites, etc.).

3.2 **Facilities:** The Government: will **NOT** provide Facilities in support of this contract/task order.

3.3 **Utilities:** The Government will **NOT** provide Utilities in support of this contract/task order. As a result, this paragraph is Not Applicable.

3.4 **Equipment:** The Government ☒will **NOT** provide Equipment in support of this contract/task order. As a result, this paragraph is Not Applicable.

3.5 **Materials**: The Government

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

3.5.1. The Government will perform and transmit all study images electronically to the contactor for diagnostic radiology interpretations along with any clinical information available to the radiologic technologist.

3.5.2 All digital images and accompanied data shall remain the property of, and subject to the exclusive control of the U.S. Government. All related reports, images, and documents prepared by the Contractor for diagnostic imaging interpretation and support in fulfillment of this contract will become the property of the U.S. Government.

3.5.3. Pertinent provider/department telephone and fax number(s) will be provided to the Contractor after Task Order award. Awarded task orders and all modifications thereafter shall be provided to the Contractor.

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 is not intended to be a comprehensive list of all Contractor furnished supplies, equipment, facilities, and services; but rather, it covers the core components that are possibly involved in a complete personnel equipment and service solution. The Contractor is required to assess the full extent of support necessary to provide the required services, equipment, and/or personnel for this contract. Compliance with the elements of this section are only relevant to the extent it is applicable to this contract.

4.2 Secret Facility Clearance: Reserved

4.3 Materials**:** Reserved

4.4 Equipment: The Contractor shall provide all necessary equipment (such as computers, servers, connectivity hardware and miscellaneous telecommunications equipment, etc.) and necessary related support to meet the requirements of this PWS. Listed below are specifications and usage guidelines related to digital image data management equipment standards and interoperability.

4.4.1. The Contractor shall use equipment in conformance with the current ACR-National Electrical Manufacturers Association DICOM standard, to ensure the enterprise-wide availability of features and performance using digital radiographic and connected equipment. The Contractor shall consider periodic upgrades incorporating the expanding features of standards and shall be included in the Contractor's ongoing QC program.

4.4.2. The Contractor shall comply with the Radiological Society of North America and Healthcare Information and Management Systems Society (HIMSS) Integrating the Healthcare Enterprise Initiative, as embodied in the available technical frameworks for all new equipment acquisitions.

4.4.3. Digital radiographic devices shall provide images that conform to the DICOM standard relating to the appropriate service class objects. These objects' header fields specify information such as accession number, patient name, identification number, date and time of examination, name of facility or institution of acquisition, type of examination, patient or body part orientation (e.g., right, left, superior, and inferior), amount and method of data compression, and total number of images acquired in the study.

4.4.4. The Contractor shall provide all Contractor-side connectivity to ensure adequate telecommunication to meet the requirements of this PWS.

4.4.5. The Contractor shall ensure its receiving computers are operational at all hours to accommodate incoming transmissions. The MTF is not required to notify the Contractor when studies have been pushed. If the system that incoming transmissions are designated to be sent to

becomes inoperable, the Contractor shall notify the MTF POC and the COR within 15 minutes with the replacement system(s)' interface information (i.e., IP address(es), ports and protocols, etc.).

4.4.6. Government Computer Access/Security. Contractor shall provide personnel who qualify for all applicable security clearance requirements to maintain access to the DHA network. The Contractor employees shall comply with the requirement to obtain the minimum-personnel security investigations as prescribed by DODI 5200.02, DOD Personnel Security Program (PSP), 3 April 2017 and Service specific requirements denoted in each TO. Submission of required security clearance documents shall be performed within 7 calendar days of contract award.

4.4.7. Information assurance, security, and confidentiality. The Contractor shall be responsible for safeguarding all medical information provided for Contractor use. The Contractor shall be responsible for maintaining patient confidentiality at all times. The Contractor shall not release patient medical information or account data, except for the purposes of this contract, without the expressed written authorization from the military treatment facility and obtain approval from the contract level KO. The Contractor shall be responsible for its employees in release of confidentiality and/or proprietary information. A proven violation of confidentiality of patient information based on a system vulnerability may be cause for termination of contract. All Contractor employees shall observe the requirements imposed on sensitive data by law, Federal Regulation, and Department of Defense (DoD)/Service specific policies and procedures. A proven violation of confidentiality of patient information by a contracted radiologist shall be cause for termination of employment on contract performance. All individually identifiable health records shall be treated with the strictest confidentiality. The Contractor shall comply with the Federal Privacy Act, 38, USC 5701, and 38 USC 7332.

4.4.7.1. The Contractor shall safeguard all DoD information. The Contractor shall not disclose or cause to be disseminated any information concerning the operation of the MTF that could increase the possibility of a breach in security or interrupt the continuity of operations, or which breaches the requirements of the Federal Privacy Act of 1974. All financial, statistical, personnel, and technical data furnished, produced, or otherwise available to the Contractor during the performance of this contract are considered confidential business information and shall not be used for purposes other than performance of work under this contract. The Contractor shall not release any of the above information without prior written consent of the TOKO or ACO, as applicable. The Contractor shall not use patient care rendered pursuant to this contract as part of a study, research project, or publication. The Contractor shall adhere to standards pertaining to the access of all patient information laws and regulations. The Contractor shall prepare forms, reports, and documents as required IAW established MTF regulations and guidelines.

4.4.7.2. The Contractor shall store all collected and/or analyzed data in an electronically, secure manner to prevent disclosure to unauthorized parties and for the purpose of making such data available to the Government as needed. The Contractor shall retain any copies, paper or electronic information once the work is completed, for a period of 3 years after final payment. IT Services in form of commercial cloud computing services must comply with DoD cloud computing policy and procedural guidance as published.

4.4.7.3. IT Services may be under contract from a commercial entity that has been authorized by a DoD or other U.S. Government agency (e.g., a commercial cloud service authorized by the Federal Risk and Authorization Management Program (FEDRAMP) Joint Authorization Board (JAB).) In this case, the Government will leverage an existing authorization and maximize reuse of the existing authorization documentation to support a new authorization by a DHA Authorizing Official (AO). If DHA determines there are inadequate security measures in place for establishing an acceptable level of risk the DoD organization may negotiate with the IT service provider for additional security measures or security-related information. Upon assessment and approval of all newly included security measures and the documentation of all applicable security measures in the contract agreement with the IT Service provider, the DHA AO issues an Authorization.

4.4.7.4. The Government will maintain data rights to all documents/material produced under this contract. All documents and materials produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/ copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the Contractor without written permission from the KO. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

4.5 **Facilities:** The Contractor shall provide all necessary facilities to support the distances/connectivity and necessary related support to meet the requirements of this PWS.

4.6 **Services:** The Contractor shall provide the services below:

4.6.1. The Contractor shall be required to obtain VPN/B2B access to connect to the Government Local Access Network (LAN) and must communicate with the network using FHIR, DICOM, HL7, and HTTPS.

4.6.1.1. Business-to-Business (B2B) Solution. B2B solution enables encrypted and secured communications between DHA and Contractors. The DHA enterprise architecture provides segregated access methods for Server-to-Server (S2S) and Client-to-Server (C2S) communication.
4.6.1.2 S2S allows continuous connectivity between the Contractor-and DHA-hosted servers. The Contractor shall be required to procure and install a DHA-configured and tested VPN router within your environment at all appropriate locations. The device, which will be remotely managed by DHA, will provide a controlled entry/exit point and an encrypted pathway for all communications between the Contractor and its DHA-hosted system(s). S2S communications are defined as automated processes between two systems that require always-on connectivity and affords DHA to export data to the vendor.

4.6.1.3. C2S allows the Contractor system administrators to manage and monitor those systems for which they are responsible. C2S communications are defined as any administrative function that requires administrative input (Remote Desktop, Dameware, SSH, etc.) from DHA entry point to vendor supported DHA asset only. This will be an on-demand solution and will require the

Contractor system administrator to establish a connection for each use through a DHA provided Virtual Desktop Infrastructure (VDI) using CAC and Alt Token PIV authentication.

4.6.2 Contractor Provided IT Infrastructure

4.6.2.1. 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 (SSL)/Transport Layer Security (TLS)), and all software that the contractor proposes to use to interconnect with DoD facilities.

4.6.2.2. The contractor shall configure their networks to support access to Government systems (e.g., configure ports and protocols for access) (in compliance with DISA Category Assurance List (CAL)).

4.6.2.3. 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 (NAT) will not be permitted.

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

4.6.3. The Contractor shall be responsible for network connectivity to access from their database location to the Government computer systems for the transference of interpretation reports. The contractor's system for delivering radiology reports must meet all cybersecurity requirements described in this document and also must conform to existing DoD EHR HL7 Interface Control Documents for radiology reporting.

4.6.4. Computer hardware utilized for viewing images shall be capable of resolution display quality in accordance with the current edition of the ACR–AAPM–SIIM Technical Standard for Electronic Practice of Medical Imaging**,** which can be obtained on the American College of Radiology (ACR) website. The Contractor will maintain all other applicable standards described in this document.

4.6.5. Contractor shall provide maintenance support of computer hardware and software for (6) years, or until end of IT services provided to ensure capability and submission of those maintenance records if requested by the Government.

PART 5
5.0 SPECIFIC TASKS

5.1. GENERAL DESCRIPTION OF WORK. The Contractor shall perform procedures and duties that are within the scope of commercial remote teleradiology services. The Contractor shall perform only those services for which privileges have been granted by the MTF Privileging Authority. All diagnostic radiology study interpretations shall be performed in the United States (i.e., within the 50 states and/or District of Columbia (D.C.)) or U.S. Territory. The Contractor shall perform and provide diagnostic image interpretations of radiology studies and consultations related to diagnostic imaging to members of the medical staff. The Contractor shall be capable of interpreting radiography (to include B-Reads), ultrasound, CT, MRI, nuclear medicine, bone densitometry, cone beam CT, and optionally PET/CT.

5.2. DIAGNOSTIC IMAGING STUDIES. The Contractor shall interpret diagnostic imaging studies to include Radiography, B-Read radiography, Ultrasound, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), nuclear medicine, bone densitometry, cone beam CT, and PET/CT. In accordance with American College of Radiology (ACR) practice parameters, Contractor shall review prior imaging for comparison to the maximum extent possible, if prior images are available.

5.2.1. The Contractor shall provide technical assistance in all diagnostic imaging studies and participate in protocoling an exam if input is necessary for administration of contrast agent or other issues.

5.2.2. Interpretation shall consist of medical evaluation of diagnostic imaging studies consistent with the American College of Radiology's "Practice Parameter for Communication of Diagnostic Imaging Findings". The Contractor shall provide interpretation and dictation on a daily basis for all services performed.

5.3. REPORTING STANDARDS.

5.3.1. STAT REPORTS. For STAT studies, the Contractor must provide a final diagnostic report into the Government EHR within one hour (60 minutes) of receipt of the transmitted images.

5.3.1.1. URGENT (NON-STAT) REPORTS. For urgent studies, the Contractor must provide a final diagnostic report into the Government EHR within 24 hours of receipt of the transmitted images. NOTE: B-Read radiograph/diagnostic imaging studies will ONLY be submitted as a routine report.

5.3.1.1. ROUTINE (NON-STAT) REPORTS. For routine studies, the Contractor must provide a final diagnostic report into the Government EHR within 5 business days of receipt of the transmitted images. NOTE: B-Read radiograph/diagnostic imaging studies will ONLY be submitted as a routine report.

5.3.1.1.1. B-READ RADIOGRAPH: Requests for B-Read analysis will be only submitted to the Contractor by Defense Center Public Health-Portsmouth (DCPH-P) (via the Navy Medical

Center Portsmouth Radiology Picture Archiving and Communications System (PACS)). DCPH-P will forward to the Contractor the single view chest x-ray and NAVMED Form 6260/7 (Navy Occupational Medical Surveillance Programs Roentgenographic Interpretation for Pneumoconiosis) with Section 1 completed (both items accomplished by the requesting MTF). The Contractor shall provide a signed B-Read report within five (5) days (120 hours) of receipt of the chest x-ray images and NAVMED Form 6260/7. The Contractor shall complete Sections 2, 3, 4, and 5 of the NAV Form 6260/7, and shall submit the completed form back to DCPH-P for further dissemination.

5.3.2. CONTINGENCY REPORTING. In the event a failed network connection prevents report transfer into Government EHR, a final report can be sent by facsimile, secure e-mail or other communication acceptable by the MTF within 24 hours and a final report placed into Government EHR by the Contractor within 12 hours after the network connection is reestablished.

5.3.2.1. The Contractor shall still provide ALL telephonic reporting in accordance with Paragraph 5.

5.3.3. CONSULTATION. Upon request, the Contractor shall be available telephonically to provide professional recommendations to MTF staff during coverage times and during normal business hours. The Contractor shall provide telephone numbers where the radiologist(s) can be reached, if consultation is required. The radiologist shall respond to any request for consultation via telephone within 15 minutes of initial notification. Answering services, answering machines, texting, electronic mail and pagers are not acceptable. Examples of consultation services that shall be provided by the Contractor include, but are not limited to, the following:

5.3.3.1. Consultation with DoD ordering providers to discuss imaging options and pre-study concerns.

5.3.3.2. Consultation with DoD imaging technologists and DoD radiologists.

5.3.3.3. Consultation with ordering and treating DoD providers to discuss diagnostic imaging study interpretations.

5.3.4. CRITICAL AND URGENT RESULTS.

5.3.4.1. CRITICAL AND URGENT RESULT DEFINITIONS AND REPORTING REQUIREMENTS.

5.3.4.1.1. CRITICAL RESULT DEFINITION
Critical results are any findings that suggest a potentially immediately life-threatening or grave condition that may require rapid intervention to avert harm. The interpreting radiologist will use clinical judgment to determine if new or unexpected findings suggest such conditions. Findings include, but are not limited to:

- acute intracranial hemorrhage or herniation
- unstable spinal fracture

- aortic dissection or occlusion
- pneumothorax, not previously reported
- unexplained pneumoperitoneum
- major vascular injury or active extravasation
- acute pulmonary embolism or deep venous thrombosis
- gonadal torsion
- clinically significant line/tube misplacement, not previously reported
- ectopic pregnancy
- bowel ischemia

5.3.4.1.2. CRITICAL RESULT COMMUNICATION REQUIREMENTS
Critical results require immediate, interruptive telephone communication to the ordering provider or designee with ability and authority to initiate appropriate clinical intervention and immediate communication acknowledgment. Issuing a final written report is not sufficient to fulfill this additional non-routine communication requirement. This non-routine communication must be made as soon as possible, but no later than 60 minutes from identification of potentially critical finding. It must be documented in the final report using this template with appropriate information in the bracketed sections:

Template:
CRITICAL RESULT COMMUNICATION
BY: [name of person communicating]
TO: [name of person receiving communication]
TIME/DATE COMMUNICATED: [time and date communicated including time zone]
METHOD: telephone
FINDING: []
TIME/DATE IDENTIFIED: [time and date identified including time zone]
END CRITICAL RESULT COMMUNICATION

Example:

CRITICAL RESULT COMMUNICATION
BY: John Smith
TO: Jack Adams
TIME/DATE COMMUNICATED: 0135 EST on April 7, 2020
METHOD: telephone
FINDING: acute intracranial hemorrhage
TIME/DATE IDENTIFIED: 0130 EST on April 7, 2020
END CRITICAL RESULT COMMUNICATION

5.3.4.1.3. URGENT RESULT DEFINITION
Urgent results are any new or unexpected findings that suggest conditions that could result in mortality or significant morbidity without appropriate clinical intervention or additional investigation, as determined by the radiologist, but are not life-threatening within a period of days to weeks. An example of this type of potentially urgent finding is a new or unexpected diagnosis of malignancy.

5.3.4.1.4. URGENT RESULT COMMUNICATION REQUIREMENTS
Urgent results require a non-routine communication with acknowledgment to the ordering provider or designee with ability and authority to take appropriate action to avert potential patient harm. Issuing a final written report is not sufficient to fulfill this additional non-routine communication requirement. This non-routine communication must be made as soon as possible, but no later than 7 days from finding identification. Documentation using this template in the final report is required:

Template:
URGENT RESULT COMMUNICATION
BY: [name of person communicating]
TO: [name of person receiving communication]
TIME/DATE COMMUNICATED: [time and date communicated including time zone]
METHOD: [e.g., telephone/secure message/etc.]
FINDING: []
TIME/DATE IDENTIFIED: [time and date identified including time zone]
END URGENT RESULT COMMUNICATION

Example:

URGENT RESULT COMMUNICATION
BY: John Smith
TO: Jack Adams
TIME/DATE COMMUNICATED: 2330 EST on April 7, 2020
METHOD: secure message
FINDING: suspicious pulmonary nodule
TIME/DATE IDENTIFIED: 2325 EST on April 7, 2020
END URGENT RESULT COMMUNICATION

If an asynchronous communication method such as secure message is used, an addendum acknowledging receipt of communication must be added to the final report by the contractor using this template within 3 days of receipt of communication acknowledgment. If no acknowledgement has been received within 3 days of the communication, the Contractor must communicate this to a designated government official so that the government can ensure appropriate communication and follow-up and the Contractor will document that acknowledgement by the government official using this template.

Template:
URGENT RESULT COMMUNICATION ADDENDUM
ACKNOWLEDGED BY: [name of person acknowledging communication]
TIME/DATE: [time and date of acknowledgment including time zone]
END URGENT RESULT COMMUNICATION ADDENDUM
Example:
URGENT RESULT COMMUNICATION ADDENDUM

5.3.5. CRITICAL TESTS:

5.3.5.1. CRITICAL TEST DEFINITION
Critical tests are procedures that require a faster than normal report to determine course of care. DHA defined critical tests are non-contrast head CT for emergent stroke evaluation and radiographs for evaluation of unintentionally retained foreign objects while the patient is in the operating room.

5.3.5.2. CRITICAL TEST REPORTING AND COMMUNICATION REQUIREMENTS
Critical test results must be reported and communicated as in Section 5.3.4.1.2 of this PWS except that the report and communication are required within 30 minutes of receiving images. Non-routine telephone communication is required regardless of results. Normal results still require a non-routine communication.

5.3.6. ROUTINE: Radiography; B-Reads; Ultrasound; CT; CT Cardiac/Coronary Angiography; MRI; Nuclear Medicine; Bone Density; Cone Beam CT and PET CT –

5.3.6.1. Contractor shall receive images from the MTF utilizing a secure DICOM server to server direct connection via an IPSEC VPN/B2B connection.

5.3.6.2. Teleradiology studies shall be interpreted by the Contractor on a PACS viewing station within a Contractor provided facility. Viewing stations must be configured with diagnostic radiology compliant monitors,

5.3.6.3. The Contractor shall review images and provide final interpretations in a written text report utilizing standard reporting format in accordance with the ACR Practice Parameter for Communication of Diagnostic Imaging Findings. The name of the interpreting radiologist shall be clearly noted on all reports.

5.3.6.3.1. Additionally, CT Reports shall follow applicable State specific radiation dose reporting requirements.

5.3.6.4. The radiologist shall electronically sign and finalize reports. The Contractor shall transmit and upload the final report into the Government EHR utilizing a secure HL7 server to server direct connection via an IPSEC VPN/B2B connection.

5.3.6.5. CT Cardiac/Coronary Angiography requires separate privileging. If an MTF performs these services, the Contractor shall ensure appropriately privileged staff are available for interpretation and reporting. Contractor shall be responsible of post-processing of DICOM raw data required for interpretation.

5.3.6.6. The B Reader Program aims to ensure competency in radiographic reading by evaluating the ability of readers to classify a test set of radiographs, thereby creating and maintaining a pool of qualified readers having the skills and ability to provide accurate and precise ILO classifications.

5.3.6.6.1 B-Reads Chest X-ray (radiograph, single frontal view) shall be interpreted according to specific standards set by the International Labour Office (ILO) to systematically describe and record the radiographic appearance of certain abnormalities of lung disease (pneumoconiosis) caused by the inhalation of dust particles, such as silica, coal mine dust, and asbestos.

5.3.6.7. Standard:

5.3.6.7.1. Routine (non-stat) reports. For routine studies, the Contractor must provide a final diagnostic report into the Government EHR within 5 business days of receipt of the transmitted images.

5.3.6.7.2. Consultation**.** The Contractor shall reference Section 5.3.3 of this PWS.
32

5.3.6.7.3. Critical and urgent results. The Contractor shall reference Section 5.3.4 of this PWS.

5.3.7 STAT: Radiography; Ultrasound; CT; CT Cardiac/Coronary Angiography; MRI; and Nuclear Medicine

5.3.7.1. Contractor shall receive images from the MTF utilizing a secure DICOM server to server direct connection via an IPSEC VPN/B2B connection.

5.3.7.2. Teleradiology studies shall be interpreted by the contract radiologist on a PACS viewing station within a Contractor provided facility. Viewing stations must be configured with medical grade monitors in accordance with diagnostic radiology compliant monitors,

5.3.7.3. The Contractor shall review images and provide final interpretations in a written text report utilizing standard reporting format in accordance with the ACR Practice Parameter for Communication of Diagnostic Imaging Findings. The name of the interpreting radiologist shall be clearly noted on all reports.

5.3.7.3.1. Additionally, CT Reports shall follow applicable State specific radiation dose reporting requirements.

5.3.7.4. The radiologist shall digitally/electronically sign (using DoD approved PKI) and finalize reports. The Contractor shall automatically transmit and upload the final report into the Government EHR utilizing a secure HL7 server to server direct connection via an IPSEC VPN/B2B connection.

5.3.7.5 CT Cardiac/Coronary Angiography requires evidence of appropriate training specifically for the award of these privileges. If an MTF performs these services, the Contractor shall ensure appropriately privileged staff are available for interpretation and reporting. Contractor shall be responsible of post-processing of DICOM raw data required for interpretation.

5.3.7.6. Standard**:**

5.3.7.6.1. STAT REPORTS For STAT studies, the Contractor must provide a final diagnostic report into the Government Electronic Health Record (EHR) within one hour (60 minutes) of receipt of the transmitted images.

5.3.7.6.2. CONSULTATION. The Contractor shall reference Section 5.3.3 of this PWS.

5.3.7.6.4. CRITICAL AND URGENT RESULTS. The Contractor shall reference Section 5.3.4 of this PWS

5.4. MONTHLY PROGRAM STATUS REPORT (MPSR). The Contractor shall prepare and submit to the program office a monthly program status report using applicable data elements from DI-MGMT-80555A (Program Progress Report). The MPSR is a record of all awarded task orders in the reporting window. It provides task order information such as task order number, award date, place of performance, teaming partners/subcontractor used by the Prime Contractor along with their designations, task order value, and issuing contracting office.

5.4.1 The report shall include information for all teaming partners/subcontractors. The MPSR shall also include specific information regarding quantity of studies/interpretations and compliance with task order performance objectives (i.e. turnaround time by modality and priority, etc.). At a minimum, the specific information shall include:

5.4.1.1 Volume - count of all examinations interpreted, grouped by modality and by originating MTF;

5.4.1.2 Report Turn-Around-Time - count of examinations meeting the reporting requirement, count of examinations not meeting the requirement, and median turn-around-time, grouped by modality, by priority, and by originating MTF (reporting requirement is 60 minutes for STAT exams and 24 hours for urgent exams, and 5 business days for routine exams; time interval is time from the Contractor receiving all study images until a report is finalized in the government EHR).

5.4.1.3 Critical Test Reporting - count of critical tests meeting the notification requirement, count of critical tests not meeting the notification requirement, and median reporting time for all critical tests grouped by originating MTF and critical test type (reporting requirement is 30 minutes for critical tests; time interval measured for critical test notification is the time from the contractor receiving all study images until a telephone critical result communication is received by the ordering provider); and

5.4.1.4 Critical and Urgent Result Reporting - count of critical results, urgent results, and asynchronous urgent result communication acknowledgment (or escalation to government if no ordering provider acknowledgment) meeting the notification requirements, count of critical results, urgent results, and asynchronous urgent result communication acknowledgment (or escalation to government if no ordering provider acknowledgement) not meeting the notification requirement, and median reporting time for all critical results, urgent results, and asynchronous urgent result communication acknowledgment (or escalation to government if no ordering

provider acknowledgement) grouped by modality and originating MTF (notification requirement is as soon as possible, but no later than 60 minutes from identification for critical results, no later than 7 days from finding identification for urgent results, and no later than 3 days from asynchronous urgent result communication for ordering provider acknowledgement (or escalation to government if no ordering provider acknowledgement); time interval measured for critical and synchronous urgent result communication is from finding identification until ordering provider or designee acknowledges the communication; time interval for asynchronous urgent result communication is from finding identification until the asynchronous communication to the ordering provider is made; time interval for acknowledgment of asynchronous urgent result communication is from asynchronous communication initiation to documentation of receipt of that communication by ordering provider or designee or responsible government official if escalated).

5.4.2 The initial MPSR is due NLT 45 days after contract award. The contractor shall develop the MPSR format and have it approved NLT 30 days after contract award by the IDIQ COR. Task Orders may require additional information to be reported, but the general MPSR format will remain the same across all task orders and the IDIQ. The MPSR will be submitted on the 15th of each month (or first workday after the 15th if it is a holiday, weekend or government furlough day) and include information for the previous month. The Contractor will deliver the report in electronic format to each KO, Contracting Specialist, and COR (both IDIQ and Task Order). In addition to submitting a MPSR for each task order each month, the Contractor shall submit a MPSR that aggregates the interpretation information across all task orders and the other information outlined in this paragraph, into a single MPSR for the IDIQ.

PART 6
6.0 INFORMATION TECHNOLOGY & SECURITY

6.1 All work under this contract is unclassified.

6.2 **The Automated Data Processing/Information Technology (ADP/IT) levels and position sensitivity designation for positions under this contract is:** (Requirement must be checked in order to be a requirement for this PWS.) ADP/IT I

6.2.1 ADP/IT I: Critical sensitive position (A position where the individual is responsible for the development and administration of Military Health System Information System (MHS IS)/network security programs and has the direction and control of risk analysis and/or threat assessment.)

6.3 **PII/PHI, 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.

6.4 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.

6.4.1.2 Certification: The Contractor shall ensure that personnel accessing information systems have the proper and current IA certification to perform IA functions in accordance with DoD 8570.01–M, IA Workforce Improvement Program. The Contractor shall meet the applicable IA certification requirements, including:

6.4.2 User requirements: All contractor employees that require access to Defense Health Agency Information Technology (DHA IT) must comply with the requirements of DHA-PI 8140.01, Acceptable Use of DHA IT.

6.5 **General cybersecurity requirements – Information Systems:** This section 6.5 through 6.5.12 is applicable only for those acquisitions where DHA will transmit Covered Defense

Information (CDI) for action on a contractor's IS system. The covered contractor information system shall be subject to the security requirements in DHA AI 042, "Security of Unclassified DoD Information on non-TMA Information Systems", DoDI 8582.01, "Security of Unclassified DoD Information on non-DoD Information Systems", and 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 effect at the time the solicitation is issued or as authorized by the Contracting Officer. (User will need to include all cybersecurity requirements if applicable. See DHA-IPM 18-015 https://health.mil/Reference-Center/Policies?page=4#pagingAnchor Cybersecurity Program Management).

6.5.1 The Contractor shall implement NIST SP 800-171[BRCMCDHI1], for systems that store, process, or transmit Controlled Unclassified Information (CUI) or provide security protection for such systems.

6.5.2 The contractor shall self-certify that the information system is compliant with the applicable NIST security controls annually by submission of a Security Assessment Report (SAR) and security test plan for compliance of testing security controls.

6.5.3 The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, 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.

6.5.4 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 copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.

6.5.5 If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that 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 6.5.6 through 6.5.10 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

6.5.6 Cyber Incident Reporting Requirement:

6.5.6.1 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:

6.5.6.1.1 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 information systems 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; and

6.5.6.1.2 Rapidly report cyber incidents to DoD at https://dibnet.dod.mil/portal/intranet/

6.5.6.2 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 at https://dibnet.dod.mil/portal/intranet/.

6.5.6.3 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

6.5.7 Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.

6.5.8 Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems 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.

6.5.9 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.

6.5.10 Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

6.5.11 Apply other information systems security measures when the Contractor reasonably determines that information systems 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. The vendor must make the system security plan within 5 business days upon the KO request.

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

6.5.12.1 Whenever Contractor collects, uses, copies, accesses, or stores Controlled Unclassified Information (including but not limited to PII and/or PHI) in commercial office space, Contractor must notify the DHA Cyber Security Division and the DHA Privacy and Civil Liberties Office.

6.6 **Risk Management Framework (RMF) for DoD IT:** All Information Systems (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 DoD Instruction (DoDI) 8510.01, RMF for DoD IT and comply with annual Federal Information Security Management 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 (SSP), SAR 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 KO 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) no later than 180 days after 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 RMF.

6.6.3 The contractor shall configure the information system in accordance with Defense Information System 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 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 United States Cyber Command 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 NIST security documents directed information 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 IS and PIT systems under this requirement in accordance with NIST SP 800-137.

6.7 **Commercial Cloud Computing Services:**

6.7.1 Commercial Cloud Computing Services: The Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order issued hereunder.

6.7.1.1 If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order.

6.7.1.2 The Contractor shall ensure that its employees are subject to all such access, use, and disclosure prohibitions and obligations.

6.7.1.3 These access, use, and disclosure prohibitions and obligations shall survive the expiration or termination of this contract.

6.7.1.3.1 The Contractor shall use Government-related data only to manage the operational environment that supports the government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

6.7.1.3.1.1 Records management.

6.7.1.3.2 The Contractor shall deliver to the Contracting Officer all Government data and Government-related data in the format specified in the schedule.

6.7.1.3.3 The Contractor shall dispose of Government data and Government-related data in accordance with the terms of the contract and provide the confirmation of disposition to the Contracting Officer in accordance with contract closeout procedures.

6.7.1.3.3.1 Notification of third-party access to Government data. The Contractor shall notify the Government immediately of any requests from a third party for access to Government data or Government-related data, including any warrants, seizures, or subpoenas it receives, including those from another Federal, State, or Local agency, that could result in the disclosure of any Government data to a third party. The Contractor shall cooperate with the Government to take all measures to protect Government data from any loss or unauthorized disclosure that might reasonably result from the execution of any such request, warrant, seizure, subpoena, or similar legal process.

6.7.1.3.3.2 Spillage. Upon written notification by the Government of a spillage, or the Contractor's discovery of a spillage, the Contractor shall coordinate immediately with the responsible Government official to correct the spillage in compliance with agency-specific instructions.

6.7.1.3.3.3 Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (g), in all subcontracts, including subcontracts for commercial items.

6.7.2 Commercial Cloud Computing Services: Contractors contracting for external IT services in the form of commercial cloud computing services must comply with DoD cloud computing policy and procedural guidance as published in DoD Cloud Computing Security Requirements Guide (SRG) current version.

6.7.3 Commercial Cloud Computing Services: To the maximum extent practicable, cloud computing services that are commercial items shall be acquired under the terms and conditions (e.g., license agreements, End User License Agreements (EULA). Terms of Service (TOS), or other similar legal instruments or agreements) customarily provided to the public, to the extent that such terms and conditions are consistent with Federal law and otherwise satisfy the Government's needs, including those requirements specified in this section. Any applicable service provider terms and conditions shall be incorporated into the contract (e.g., by attachment or other appropriate mechanism).

6.7.4 Commercial Cloud Computing Services: The contracting officer shall not award a contract to acquire cloud computing services from any cloud service provider (e.g., contractor or subcontractor, regardless of tier), that has not been granted provisional authorization to provide the relevant cloud computing services in accordance with the Cloud Computing SRG (version in effect at time of contract award) found at https://public.cyber.mil/. All necessary SRG requirements, including cloud access point connections and authorizations to operate, must be satisfied before the cloud computing service becomes operational.

6.7.5 Commercial Cloud Computing Services: Contractors contracting for Cloud services will only use cloud services that have been issued both a DoD Provisional Authorization

by DISA and obtained an Authority to Operate (ATO) (Reference (f)) by the DHA Authorizing Official (AO).

6.7.6 Commercial Cloud Computing Services: Non-DoD cloud services hosting CUI (Personally Identifiable Information (PII)) shall be connected to customers through a Cloud Access Point that has been approved by the DoD CIO and have a Cyber Security Service Provider (CSSP).

6.7.7 Commercial Cloud Computing Services: Cloud Service providers shall establish a security baseline in accordance with the Federal Risk Authorization and Management Program (FedRAMP) and achieve a FedRAMP (level 4-5) authorization to store/process DoD sensitive information within the Cloud Service Provider (CSP)and be compliant with DoD Cloud Computing Security Requirements Guide (SRG) current version.

6.7.8 Commercial Cloud Computing Services: The contractor shall connect to customers through a DoD Cloud Access Point (CAP) for commercial cloud services hosting CUI and comply with DoD Cloud Computing SRG current version.

6.7.9 Commercial Cloud Computing Services: The contractor shall implement DoD Cloud Computing SRG current version specific security requirements for cloud services that contain PII/Protected Health Information (PHI).

6.7.10 Commercial Cloud Computing Services: The contractor is solely responsible for the cost associated with obtaining a FedRAMP Provisional Authorization (PA) to host Federal Government missions and obtaining a DoD Provisional Authorization to Operate (P-ATO).

6.7.11 Commercial Cloud Computing Service: The Contractor shall adopt and maintain administrative, technical, and physical safeguards and controls that are required for the security level and services being provided, in accordance with the Cloud Computing SRG, (version in effect at the time of contract award).

6.8 Defense Health Agency (DHA) Cyber Logistics (CyberLOG) Cybersecurity/Risk Management (RMF) Requirements

6.8.1 New Equipment/Product systems, equipment, IT Services and software under RMF: The Contractor shall comply with References listed in this PWS.

6.8.1.1 Software patches and updates: Many enterprises within the DoD automate patch updates and software updates for operating systems and DoD standard software applications. For applications such as databases and developed applications, updates are scheduled. The Contractor shall notify the assigned CyberLOG analyst of any updates/changes to the system prior to installation, to include but not limited to software updates, Operating System, or Application upgrades, patches, addition/removal of components. If the CyberLOG analyst is unknown, the Contractor shall submit all requests to dha.ncr.mbx.mde-cyber-support@health.mil. Software updates will be analyzed by the Government to determine if

reauthorization is required by Department of Defense Instruction (DoDI) 8510.01 Risk Framework (RMF) for DoD Information Technology (IT). Patches normally address bug fixes and cybersecurity issues. Applying patches usually does not trigger reauthorization. Per the DoDI 8500.01 Cybersecurity, Enclosure 3, paragraph 9.b. (11), "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 Information Assurance (IA) and IA-Enabled Information Technology Products*, June 2013, as amended."

6.8.1.2 Contractor 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. Contractor is required to continually maintain its products, mitigating vulnerabilities and distributing fixes to licensed users.

6.8.1.3 Reauthorization in accordance with DoD RMF requirements: Per DoDI 8510.01, Enclosure 6, para 2.f.(6).(a), "In accordance with Appendix III of Office of Management and Budget (OMB) Circular A-130, systems must be reassessed and reauthorized every 3 years or as a result of a system update that negatively affects the security posture (whichever is less)." Program Offices or appropriate logistics 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.

6.8.1.4 The Contractor shall maintain all equipment/product versions provided pursuant to this contract, to include the supported operating system, by issuing patches/updates to mitigate vulnerabilities [e.g., Information Assurance Vulnerability Alerts (IAVA) or Information Assurance Vulnerability Bulletins (IAVB)] and network security configurations [e.g., Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs)]. The Contractor must adhere to DHA guidance for remediation or mitigation of vulnerabilities associated with the equipment/product. Contractor shall be responsible for providing CYBERSECURITY maintenance support for five (5) years. The Contractor shall patch its equipment throughout its lifecycle.

6.9 Pricing for Cybersecurity: Contractor shall support elements of the Cybersecurity lifecycle, to include:

6.9.1 Achieving the initial Authority to Operate (ATO) and maintaining it during the period of performance.

6.9.2 Contractor shall update and upgrade equipment (hardware and software) to maintain the ATO throughout the period of performance. 6.9.3 Maintenance and upgrades: Contractor shall comply with the DHA Cybersecurity requirements as outlined in this PWS for all systems and medical devices, unless an exception has been granted for a system by the Government prior to award/Task Order issuance.

6.10 DHA Cybersecurity/Risk Management Framework (RMF) Requirements

6.10.1 System Security Requirements

6.10.1.1 The Contractor shall complete and submit all sections of the Medical Device Equipment Risk Assessment (MDERA Questionnaire) (See attachment in para 7.5 of this PWS), provided by the Government, with proposal. Additionally, a vulnerability assessment/report is required from a NESSUS scanner as this is the DoD standard.

Contractor shall provide a fully credentialed NESSUS scan with one month post award and because these results are only good for 60 days a Final NESSUS scan Proposal will be submitted within 3 months post award (per Table F1). Contractor shall provide monthly Nessus scans by the tenth (10th) day of the month after the system has been accredited.

6.10.1.2 Contractor shall comply with security regulations and guidance listed in Part 6: Cybersecurity Regulations and Guidance and all RMF requirements.

6.10.1.3 The Contractor's device or system shall pass pre-validation technical screening (vulnerability scans utilizing NESSUS, Security Content Automation Protocol (SCAP) scans, and Security Technical Implementation Guides (STIGs) checklists) within 3 months of contract award. All technical scans shall be provided by the Contractor to the Government COR for review. The Contractor's Medical Device and Equipment (MDE) shall pass fully credentialed screening given DHA approved template. Successful pre-validation technical screening shall meet the Cybersecurity criteria listed below:

6.10.1.4 No unmitigated Very High or High Severity/Category I (CAT I), vulnerabilities as described in the appropriate Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs) located on http://iase.disa.mil/stigs/Pages/index.aspx

6.10.1.5 No unmitigated Moderate Severity/Category II (CAT II), vulnerabilities described in the appropriate DISA STIGs located on http://iase.disa.mil/stigs/Pages/index.aspx

6.10.1.6 No unmitigated Very High or High Severity/ Category I (CAT I) vulnerabilities from Nessus vulnerability scans.

6.10.1.7 No unmitigated Moderate Severity/Category II (CAT II) vulnerabilities from Nessus vulnerability scans.

6.10.1.8 The Government will provide templates of all technical documentation no later than five (5) business days from date of initial request from the Contractor. Initial response and acknowledgement from the Contractor is due within five (5) business days of delivery of the templates. The Contractor shall remit all requested technical documents to the Government no later than one hundred and thirty (130) calendar/business days from award of the initial (Base Year) Task Order.

6.10.1.9 The Contractor shall mitigate all Very High, High, and Moderate Severity/CAT I, and CAT II vulnerabilities discovered during the RMF Assessment process according to the associated Plan of Action & Milestone (POA&M), provided by the Government.

6.10.1.10 The Contractor shall provide a Point of Contact (POC) responsible for the cybersecurity of the Contractor's device or system, throughout the lifecycle of the system. The Contractor shall provide Subject Matter Experts (SMEs) to support all assessments of the products and materials outlined in Table F1.

6.10.1.11 For all equipment requiring a full Independent Verification and Validation (IV&V) test, the Contractor shall not make any hardware installation until the Basic Contract COR has completed a self-assessment and the IV&V has been completed. IV&V cannot be scheduled until all documentation requirements, and technical requirements have been completed and approved by the Government. Additionally, all identified POA&Ms must have been identified, and been appropriately mitigated to reduce the risk to the Government network and Protected Health Information (PHI)/Personally Identifiable Information (PII)/For Official Use Only (FOUO) data housed within the system. Delivery may take place prior to this milestone (IV&V scheduling) only if written permission is provided by the KO.

6.10.1.12 For all equipment requiring an Assess Only certification, the Contractor shall not access any Government system until the Basic Contract COR has completed a self-assessment, and the system has been accepted for an Assess Only ATO/APL. Submission cannot be scheduled until all documentation requirements, and technical requirements have been completed and approved by the Government. Additionally, all POA&Ms must have been identified, and been appropriately mitigated to reduce the risk to the Government network and

PHI/PII/FOUO data housed within the system. The Contractor must receive written confirmation from the Basic Contract COR or KO that the system has been submitted for an Assess Only ATO/APL and that the Contractor may proceed with delivery. Delivery may take place prior to this milestone only if written permission is provided by the KO.

6.10.1.13 The Contractor shall obtain a recommendation of ATO from a Government-appointed third party validator within six (6) months of contract award for technologies processed through an Assessment & Authorization (A&A) pending all timelines and requirements are met and there are not any delays from the vendor or government. Additionally, the Contractor shall obtain an authorization from a Government official to be added to an APL for systems/devices processed through an RMF Assess Only.

6.10.1.14 Prior to final installation, the Contractor shall ensure that the installed device matches the DoD authorized configuration. The Contractor shall coordinate running Nessus and SCAP scans with the site and the assigned CyberLOG Analyst to verify compliance. If the CyberLOG analyst is unknown, the Contractor shall submit all requests to dha.ncr.mbx.mde-cyber-support@health.mil Any deviations will require the Contractor to bring the system into compliance prior to performance.

6.10.1.15 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 the period of performance.

6.10.1.16 The Contractor shall establish appropriate administrative and technical safeguards to ensure the confidentiality, integrity, and availability of Government data under their control.

6.10.1.17 The Contractor shall notify the COR and KO in writing with any inabilities to comply with DoD security requirements. Contractor shall provide timelines required to address any vulnerabilities in question. The vulnerabilities within the POA&MS have Timelines (Milestones) in which the vulnerabilities are to be fixed/mitigated. For each vulnerability there is a timeline associated with it unless it is a risk accepted by the Authorizing Official which requires justification regarding why the vulnerability cannot be fixed and other mitigating factors (defense in depth mitigations) have been implemented to minimize the exposure of the vulnerability.

6.10.1.18 The Contractor shall contact the MTF specific IA/RMF Office Representative, provided by the Government, no later than five (5) business days after Task Order issuance for teleradiology services, to start the process. Failure to do so would be considered a Contractor-caused delay.

6.10.1.19 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.

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

6.10.1.20 The contractor shall be able to demonstrate or provide documentation to prove that their product is IPv6 capable.

6.11 RMF Assessment Timeframes

6.11.1 Required Timeframes: The Contractor shall complete its required actions within the referenced timeframes in the Table F1 below. If the Contractor has completed all required actions in a timely and acceptable manner while the Government experiences delays, the Contractor shall be given additional time for future actions corresponding to the amount of Government delay.

TABLE F1

Contractor Requirements:	Initial Draft Date Due	Final Date Due

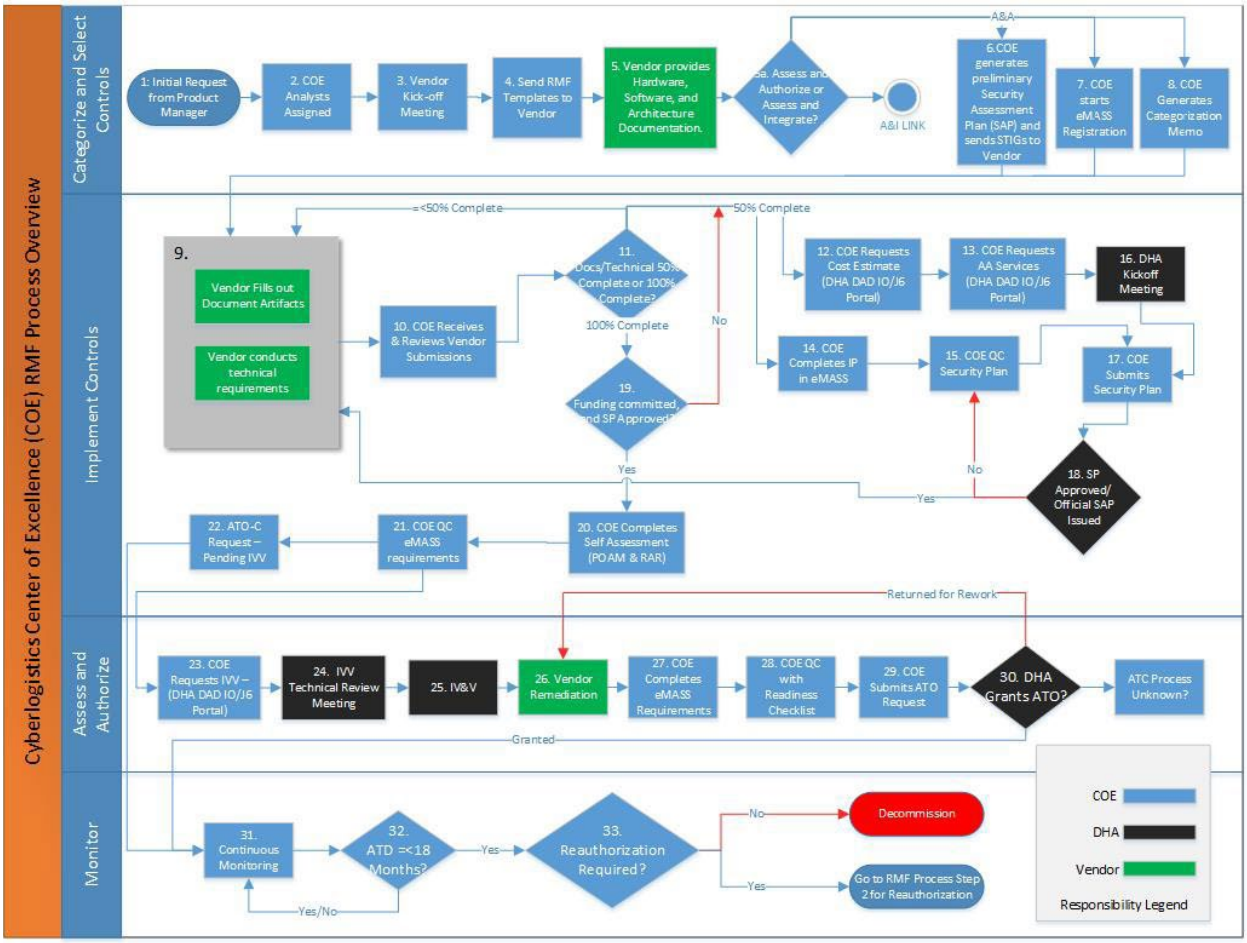
Contractor to contact Cyber Security POC (provided by the Government) dha.ncr.mbx.mde-cyber-support@health.mil	5 business days post Contract award	
Hardware/Software/Architecture Documents	15 business days post Contract award	20 business days post award
RMF Documentation Production	6 weeks post Contract award	3 months post award
Technical Nessus Scans	1 month post Contract award	3 months post award
Technical STIG Checklists	1 month post Contract award	3 months post award
Technical SCAP	1 month post Contract award	3 months post award

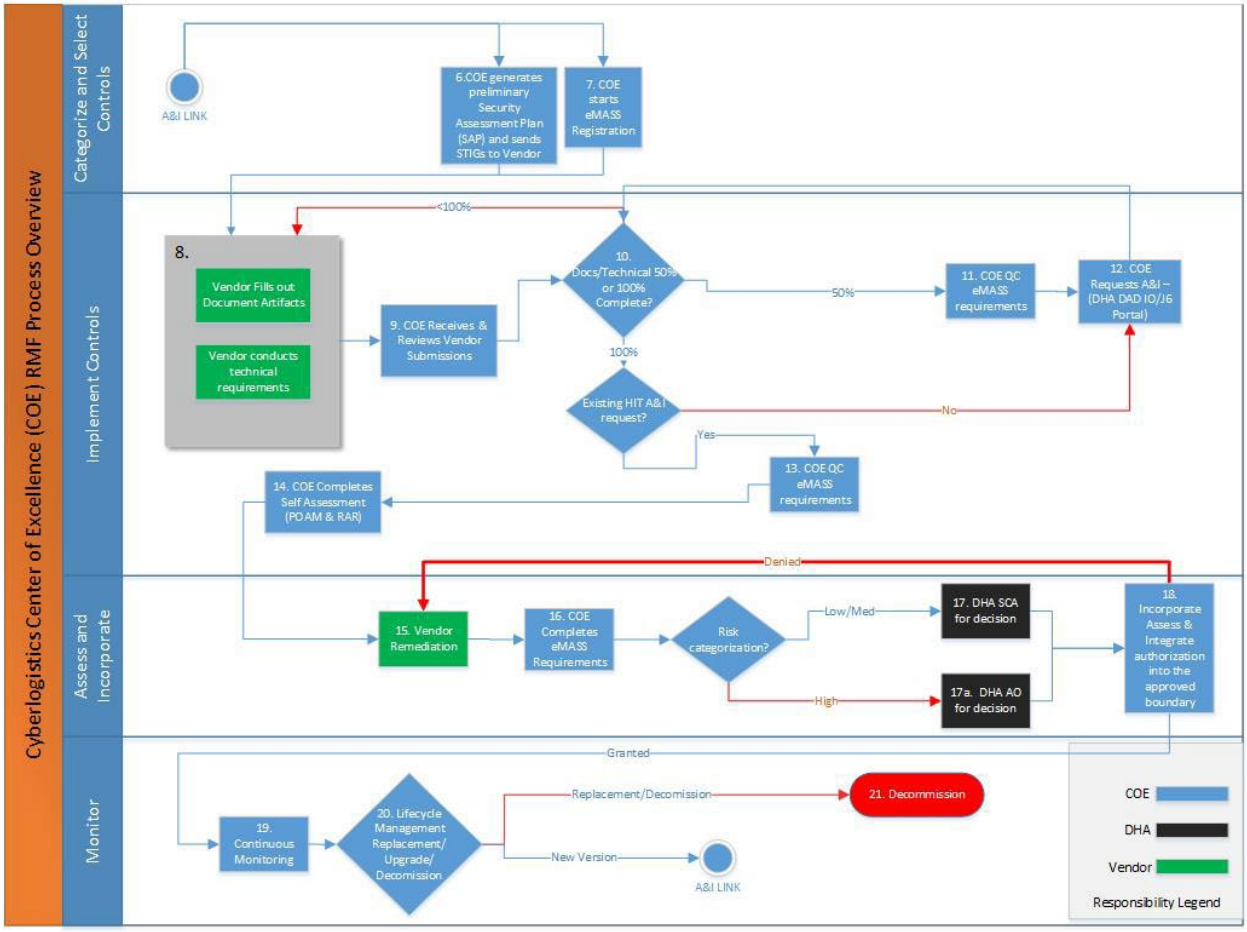
6.11.2 Required Timeframes: The Government shall complete its required actions within the referenced timeframes in the Table F2 below. If the Contractor has completed all required actions in a timely and acceptable manner while the Government experiences delays, the vendor may be given additional time for future actions corresponding to the amount of Government delay.

TABLE F2

Government Requirements	Initial Draft Date Due	Final Date Due
Assessment and Authorization (A&A) Kickoff (may be virtual) Meeting	15 business days post award	-
Security Assessment Plan Generation	20 business days post award of Contract or Task Order or both	30 business days post award
RMF Templates sent to Contractor	5 business days post Contractor request	
Copies of Applicable STIGs sent to Contractor	17 business days post award of Contract or Task Order or both?	30 days post award
Authorization to Operate with Conditions (ATO-C) Recommendation	ATO-C recommendation submitted to 3rd party validator 2 weeks after final documentation/technical scans received	
Independent Verification and Validation (IV&V) Scheduling	Scheduling request to 3rd party validator 3 weeks after final documentation/technical scans received	

6.11.3 Informational Overview of the RMF Process: The following diagrams provide a summary overview of the entire process to obtain approval under DHA Cybersecurity requirements. These diagrams are for informational purposes only, are not contractually binding, and subject to change without notice.


Cyberlogistics Center of Excellence (COE) RMF Process Overview
Categorize and Select Controls
Implement Controls
Assess and Authorize
Monitor
1: Initial Request from Product Manager
2. COE Analysts Assigned
3. Vendor Kick-off Meeting
4. Send RMF Templates to Vendor
5. Vendor provides Hardware, Software, and Architecture Documentation.
5a. Assess and Authorize or Assess and Integrate?
A&I LINK
A&A
6.COE generates preliminary Security Assessment Plan (SAP) and sends STIGs to Vendor
7. COE starts eMASS Registration
8. COE Generates Categorization Memo
=<50% Complete
50% Complete
9.
Vendor Fills out Document Artifacts
Vendor conducts technical requirements
10. COE Receives & Reviews Vendor Submissions
11. Docs/Technical 50% Complete or 100% Complete?
100% Complete
No
12. COE Requests Cost Estimate (DHA DAD IO/J6 Portal)
13. COE Requests AA Services (DHA DAD IO/J6 Portal)
16. DHA Kickoff Meeting
14. COE Completes IP in eMASS
15. COE QC Security Plan
17. COE Submits Security Plan
19. Funding committed, and SP Approved?
Yes
No
Yes
18. SP Approved/ Official SAP Issued
22. ATO-C Request – Pending IVV
21. COE QC eMASS requirements
20. COE Completes Self Assessment (POAM & RAR)
Returned for Rework
23. COE Requests IVV – (DHA DAD IO/J6 Portal)
24. IVV Technical Review Meeting
25. IV&V
26. Vendor Remediation
27. COE Completes eMASS Requirements
28. COE QC with Readiness Checklist
29. COE Submits ATO Request
30. DHA Grants ATO?
ATC Process Unknown?
Granted
31. Continuous Monitoring
32. ATD =<18 Months?
Yes
33. Reauthorization Required?
No
Decommission
Yes
Go to RMF Process Step 2 for Reauthorization
Yes/No
COE
DHA
Vendor
Responsibility Legend



Note: Not all above actions occur in a sequential manner, as some actions may be worked concurrently.

6.12 Assessment and Authorization (A&A)

6.12.1 The Contractor shall provide hardware/software lists, architecture drawings, and workflow drawings and all other RMF-required documentation for review and approval in accordance with Table F1.

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

6.12.3 The Contractor shall provide any additional documentation required by the Government for completion of the A&A process as specified after Contract award.

6.12.4. The Contractor shall provide technical scans in accordance with Table F1.

6.12.5 The Contractor shall provide updated technical scans on a monthly basis, on the 10th day of each month until an ATO is granted or the product is added to the APL.

6.12.6. In accordance with DoD 8582.01 Security of Unclassified DoD Information on Non-DoD Information Systems, incorporating Change 1, October 27, 2017 Section 2.0 INFORMATION SAFEGUARDS, the Contractor shall ensure that the selected MDE is capable of supporting the use of DISA approved intrusion detection and prevention, antivirus, and anti-malware applications that are approved at the time of the ATO or APL issuance. The Contractor device or system 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 (DLP), Intrusion Prevention System (IPS), Antivirus, etc.) without performance degradation of the Contractor device or system. In cases where the operation of security applications are not technically achievable, the Contractor shall provide detailed justification and a POA&M describing steps towards compliance with this requirement.

6.13 Privileged User Training and Certification Requirements

6.13.1. If a Contractor needs to connect remotely then they are required to use the DHA Business-To-Business (B2B) gateway. In order to access Government networks to maintain, analyze, etc., their equipment/products, they must adhere to the following requirements:

6.13.1.1. Information Assurance Contractor Training and Certification. All Contractors requiring access to their system for administrative/maintenance support of systems/applications on the DoD network shall meet DoD requirements for a privileged-level account before being granted a network account. Requirements include:

6.13.1.2. Cyber (Information assurance (IA)/information technology (IT)) certification. Per DoD 8570.01-M DFARS 252.239.7001, the contractor employees supporting Cyber (IA/IT) functions shall be appropriately certified. Contractors shall be defined at Information Assurance Technical level II (IAT-II) and be required to meet minimum Professional Baseline certifications before access will be granted. Contractors shall be given six (6) months to meet Computer Environment (CE) and Cyber Security Fundamental training requirements. Not meeting the requirements in accordance with DoD 8570.01-M will result in the contractor account and access being ‘Disabled’ or ‘Deleted’ until such time as the conditions of this contract are met.

6.13.1.3. Background Investigation. A T3 investigation is required. Adjudication: Position of Trust is the minimum eligibility for ADP/IAT-II which is required for B2B Gateway/DoD network access. A completed investigation and adjudication are required for remote access through the B2B.

6.13.1.4. Professional Baseline Certification. The minimum Professional Baseline certification for IAT-II is CompTIA Security+ or equivalent listed in DoD 8570. Higher certifications (GSCL, CISM, CISSP, etc.) will also satisfy this requirement.

6.13.1.5. Computer Environment (CE) Certification. The CE certifications are determined by the role of the Contractor and shall be met within six (6) months of delivery order issuance in accordance with DoD 8570.01-M.

6.13.1.6. Two-Factor Authentication. Contractors shall authenticate using two-factor authentication. The only method for authenticating is the Common Access Card (CAC).

6.13.1.7. Network Account Request Package (Authorized & Privileged). The Contractor shall submit a request package through either the facility Provost Marshall Office in conjunction with the facility Information Management Department (for Contractors requiring on-site access), or through the Information Assurance/Cyber Security Branch (for Contractors requiring remote access to a DHA network). Remote access must be through a DISA B2B solution.

6.13.1.8. The CYBERSECURITY Training. DoD Cyber Awareness Challenge Training shall be completed by all Contractor employees and subcontractor employees prior to issuance of network access and annually thereafter. DoD Cyber Awareness Challenge Training is available at the following website: https://iase.disa.mil/eta/Pages/online-catalog.aspx

6.13.1.9. Personally Identifiable Information Training (PII). DoD PII Training shall be completed by all Contractor employees and subcontractor employees prior to issuance of network access and annually thereafter. DoD PII Training is available at the following website: https://iase.disa.mil/eta/Pages/index.aspx

6.13.1.10. Health Insurance Portability and Accountability Act (HIPAA) Training. DoD HIPAA Training shall be completed by all Contractor employees and subcontractor employees prior to issuance of network access and annually thereafter. DoD HIPAA Training is available at the following website: https://jkodirect.jten.mil/Atlas2/page/login/Login.jsf?ORG=MHS

6.13.1.11. Acceptable Use Policy (AUP). Contractor shall sign/acknowledge the DHA Standard Acceptable Use Policy (AUP) prior to being granted a DHA network account. The DHA Standard AUP is available at the following website: https://health.mil/Reference-Center/Policies?query=Acceptable%20Use

6.13.1.12. In addition to those specified in this PWS, the Contractor is responsible for adhering to certification and qualification requirements for IAT-II specified in Attachment D and Section 7.1 of this PWS.

6.14 Continuous Monitoring/Risk Management.

6.14.1. 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.

6.14.2. The Contractor shall maintain the authorized security configuration and notify the Government within forty-eight (48) hours of any changes for review. A major upgrade such as

major software or hardware revision must be reassessed for ATO or addition to the approved products list. 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.

6.14.3. The Contractor shall ensure the Contractor's device or system is in compliance with the Department of Defense (DoD) Information Assurance Vulnerability Management (IAVM) program.

6.14.4. The Contractor shall maintain the system or device and update to comply with updated STIGs made available by the Government within three (3) months of notification by the Government.

6.14.5. The Contractor shall provide vulnerability and configuration scan results to the Government on a monthly basis. The Contractor shall provide raw scan results and administrative reports no later than the tenth (10th) calendar day of each month.

6.14.6. 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.

6.14.7. The Contractor shall submit to the Government for approval, all mitigation plans that addresses any open vulnerabilities.

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

6.14.9. The Contractor shall use the Government-approved method for remote access administration (DISA B2B) of the system or device.

PART 7
7.0 ATTACHMENTS/APPENDICES

7.1 Contractor CAC Request Process
DHA CAC Request Process.pdfDMDC TASS Application.xlsxDHA_FSO Guide_CTR Request

7.2 DHA's Contractor Training Instructions
Contractor Employee Mandatory Training (0

7.3 CHCS Interface Control Document
Appendix H_CHCS Interface Control Do

7.4 MHS Genesis Interface Control Document
Appendix I_MHS GENESIS Interface Co

7.5 MDERA Questionnaire
Attachment 2 Joint Medical Device Cybe

7.6 DHA Onboarding Checklist For Contractor Employees. The most up to date DHA Onboarding checklist may be found at:
https://info.health.mil/sites/DOP/OnboardingCtr/Contractor_OnBoarding_Checklist.pdf
Contractor_OnBoarding_Checklist.pdf

7.7. NAVMED Form 6260/7 Navy Occupational Medical Surveillance Programs Roentgenographic Interpretation for Pneumoconioses
NAVMED Form 62607 - B READ FORM

7.7 Appendices
A. Performance Requirements Summary (PRS)
B. Estimated Workload Data
C. Deliverable Schedule
D. Instructions for Contractor Access DoD IT Systems and the Common Access Card
E. List Of Excluded Individuals And Entities (LEIE)
F. Personally Identifiable Information, Protected Health Information, And Federal Information Requirements

Attachment 4, FRCS Responsibility Matrix

Attachment 4-FRCS Responsibility Matrix.p

Attachment 5, Risk Assessment Timeframes

Attachment 5-Risk Assessment Timeftam

APPENDIX A
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 Rating Definitions

The performance ratings below reflect definitions at FAR 42.1503 Table 42-1. The COR will use these rating to evaluate the quality of contractor's performance.

Performance Rating	**Definition**
Exceptional	Performance meets contractual requirements and exceeds many to the government's benefit. The contractual performance of the element or sub-element being evaluated was accomplished with few minor problems for which corrective actions taken by the contractor were highly effective.
Very Good	Performance meets contractual requirements and exceeds some to the Government's benefit. The contractual performance of the element or sub-element being evaluated was accomplished with some minor problems for which corrective actions taken by the contractor were effective.
Satisfactory	Performance meets contractual requirements. The contractual performance of the element or sub-element contains some minor problems for which corrective actions taken by the contractor appear or were satisfactory.
Marginal	Performance does not meet some contractual requirements. The contractual performance of the element or sub-element being evaluated reflects a serious problem for which the contractor has not yet identified corrective actions. The contractor's proposed actions appear only marginally effective or were not fully implemented.
Unsatisfactory	Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance of the element or sub-element contains a serious problem(s) for which the contractor's corrective actions appear or were ineffective.

Note 1: Plus or minus signs may be used to indicate an improving (+) or worsening (-) trend insufficient to change the evaluation status.

Note 2: N/A (not applicable) should be used if the ratings are not going to be applied to a particular area for evaluation.

Performance Requirements Summary (PRS)				
Performance Requirement	Performance Standard	Acceptable Quality Level (AQL)	Surveillance Method	
Licensure/Credentials	IAW PWS Para 1.12	100% Compliance	Periodic Inspection, Random Inspection	
Submit Credentials/Privileging Packets	IAW PWS Para 1.13 as defined at TO Award	100% Compliance	100% Inspection, Periodic Inspection, Random Inspection	
Consultation	Within 15 minutes of initial notification. IAW PWS 5.3.3.	100% Compliance	Periodic Inspection, Random Inspection	
Critical Test Result Non-Routine Communication	Within 30 minutes of receipt of images. IAW PWS Para 5.3.5.	100% Compliance	100% Inspection, Periodic Inspection, Random Inspection	
Critical Result Non-Routine Communication	Within 60 minutes of discovery. IAW PWS Para 5.3.4.	100% Compliance	100% Inspection, Periodic Inspection, Random Inspection	
Urgent Result Non-Routine Communication	Within 7 days of discovery. IAW PWS Para 5.3.4.	100% Compliance	100% Inspection, Periodic Inspection, Random Inspection	
Urgent Result Non-Routine Communication Acknowledgment	Within 3 days of urgent result non-routine communication. IAW PWS Para 5.3.4.	100% Compliance	100% Inspection, Periodic Inspection, Random Inspection	
Provide a final ROUTINE Diagnostic	Within 24 hours of receipt of images. IAW	99% Compliance	Period Inspection, Random	

Report to Government EHR	PWS Para 5.3.6.6.1.		Inspection, and/or Customer Feedback	
Provide a final URGENT Diagnostic Report to Government EHR	Within 24 hours of receipt of images. IAW PWS Para 5.3.6.6.1.	99% Compliance	Period Inspection, Random Inspection, and/or Customer Feedback	Non-compliance with this performance requirement could result in a less than satisfactory Contractor Performance Assessment Reporting System (CPARS) rating.
Provide a final STAT Diagnostic Report to Government EHR	Within 60 minutes of receipt of images. IAW PWS 5.3.7.6.1	99% Compliance	Period Inspection, Random Inspection, and/or Customer Feedback	
Provide a final Critical Test Diagnostic Report to Government EHR	Within 30 minutes of receipt of images. IAW PWS para 5.3.5.	100% Compliance	100% Inspection, Periodic Inspection, Random Inspection	
Provide a B-Read final diagnostic report to the Government EHR	Within five (5) days of receipt of images and NAV Form 6260/7 IAW PWS para 5.3.1.1.1.	97% Compliance	100% Inspection, Periodic Inspection, Random Inspection	

DELIVERABLES SCHEDULE

Deliverable	Frequency	Medium/Format	Submit To	Applicable to:
CDRL A001 – Quality Control Plan	Within 30 days of task order award	Contractor's discretion	CDRL A001 to	All, See PWS 1.10.1

			Contracting Officer	
Transition-in, Transition-out CDRLs if a Government requirement for this contract.		Transition-in: Transition-out: 6 months prior to close of contract or unexercised option.	1.6.1.1 and 1.6.1.2.	
Monthly Program Status Report	Format approved by Government NLT 30 days after contract award. Initial report due NLT 45 days after contract award, with subsequent monthly reports due on the 15th of each month (or first workday after the 15th if it is a holiday, weekend or government furlough day)	Electronic Copy; Format to be at contractor's discretion and approved by Government	COR Program Office MTF	5.4
Peer Review	Quarterly by the 10th day of the month; within 7 calendar days of Government request	Electronic Copy; Format to be at contractor's discretion and approved by Government	COR Program Office MTF Privileging Authority	1.10.3
Provider Listing	Prior to providing services to each MTF; within 24 hours of contract	Electronic Copy; Format to be at contractor's discretion and approved by Government	COR Program Office MTF Privileging Authority	1.11.3

	radiologist changes			
Provider Activity Report	Semi-annually NLT 10th day of month	Electronic Copy; Format to be at contractor's discretion and approved by Government	COR Program Office MTF Privileging Authority	1.11.3

Requirements for counting of examinations for CLIN charges described by modality.
1.1. Radiographs. A single body region, regardless of number of views, counts once.

1.2. Examinations that cover multiple body parts count once for each region examined. EXCEPTIONS: metastatic and non-accidental trauma bone surveys count once, acute abdomen series covering chest and abdomen/pelvis counts once. EXAMPLES: bilateral 3-view feet count twice, 5-view lumbar spine counts once.
1.3. CT. Each body region counts once. EXCEPTION: CT abdomen/pelvis counts once. Examples: Combined CT head/CT neck counts twice, CT chest/abdomen/pelvis counts twice (once for CT chest and once for CT abdomen/pelvis), CT liver with pre-contrast and multiple post-contrast phases counts once.

1.4. US. Each body region counts once. Additional Doppler evaluation of same body region is not counted an additional time. EXAMPLES: US right upper abdominal quadrant including Doppler evaluation of portal and hepatic veins counts once, bilateral lower extremity Doppler to evaluate DVT counts twice, US pelvis using both endovaginal and transabdominal approaches and including Doppler counts once.

1.5. MRI. Each MRI body region counts once. MRA and MRI of same region count twice.

APPENDIX E
LIST OF EXCLUDED INDIVIDUALS AND ENTITIES (LEIE)

The Contractor shall not employ or contract with any individual or entity (hereinafter collectively referred to as "person") to provide items or services that will be included in invoices submitted to the Government under this contract if such person is listed on the Department of Health and Human Services (HHS) Office of the Inspector General (OIG) List of Excluded Individuals and Entities (LEIE) or the TRICARE Sanctioned Provider List. The Government is legally prohibited from paying for provision of items or services by such persons. The prohibition extends to services beyond direct patient care, such as services of persons in executive or leadership roles and administrative and management services, whether or not such services are billed separately. The LEIE may be found at http://oig.hhs.gov/fraud/exclusions.asp, and the TRICARE Sanctioned Provider list at http://www.health.mil/Military-Health-Topics/Access-Cost-Quality-and-Safety/Quality-And-Safety-of-Healthcare/Program-Integrity/Sanctioned-Providers. The LEIE and TRICARE Sanctioned Provider List are hereinafter collectively referred to as "the Lists."

Prior to start of contract performance, the Contractor shall (a) query the Lists to determine whether the name of any person the Contractor employs or contracts with to provide services or items for which payment may be made under this contract appears on the Lists, and (b) certify to the KO that the Contractor has queried the Lists and no such names appear on either of the Lists.

During performance of the contract, and prior to persons other than those whose names were queried in accordance with paragraph 2, above, (hereinafter "new persons") providing services or items under the contract, the Contractor shall (a) query the Lists as in paragraph 2, and (b) certify to the KO that the names of such new persons do not appear on either of the Lists.

The Contractor is advised that during performance of the contract, MTF personnel will perform a recurrent recheck of the names of Contractor personnel against the Lists. The Government will notify the Contractor in the event any Contractor personnel appear on either of the Lists.

Should any person providing items or services under the contract appear on either of the lists at any time during contract performance, the Contractor shall (a) in cases where the Contractor identified the person, notify the KO, and (b) promptly remove that person from the contract.

Violation of any aspect of the above paragraphs shall be considered a material breach of the contract and may result in termination of the contract.
The Contractor is further advised that, in accordance with Civil Monetary Penalties Law [CMP] (codified at 42 USC § 1320a-7a):

There are steep civil monetary penalties associated with billing the Government for providing items or services by a person on either of the Lists, and with failing to return to the Government any overpayments received for provision of such items or services.

Billing under the contract for provision of items or services by a person on either List may also result in exclusion of the person that employs or contracts with such person.

HHS OIG has issued a Special Advisory Bulletin on the Effect of Exclusion from Participation in Federal Health Care Programs with additional information on the CMP. The Special Advisory Bulletin may be found at http://oig.hhs.gov/exclusions/files/sab-05092013.pdf.
(End of LEIE Clause)