



Department of Defense
Defense Health Agency
Performance Work Statement

LivaNova Autotransfusion Unit Service Maintenance

DSS Anesthesiology Service

PART 1
1.0 GENERAL INFORMATION

1.1 This is a **non-personal services contract to provide** Preventive Maintenance services for (2) LivaNova Autotransfusion Units.

1.2 **Description of services/introduction:** The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Preventive Maintenance and repair services for 2 government-owned LivaNova Autotransfusion Units as defined in this Performance Work Statement (PWS) except for those items specified as government furnished property and services. The contractor shall perform to the standards in this PWS.

- a. **1.3 Background:** Perform Preventative Maintenance in accordance with OEM specifications.
- b. Ensure that only FULLY QUALIFIED ENGINEERS and TECHNICIANS who has gone through original equipment manufacturer (OEM) or comparable third-party service schools for the above-mentioned equipment, shall be employed in the performance of any and all work performed under this contract. Upon request, the contractor shall provide training certificates (or notarized copies) to the Material Management Department.

1.4 Objectives:

Conduct full services to include preventative maintenance of the OEM standards, and all local, state and federal policies.

1.5 **Scope:** All services, materials, and equipment will be provided by contractor to conduct Preventive Maintenance and repair services for government-owned Autotransfusion Units located at NMRTC San Diego.

1.6 Period of Performance (PoP):

Base year: 21 OCT 2026 TO 20 OCT 2027

OY1: 21 OCT 2027 TO 20 OCT 2028

OY2: 21 OCT 2028 TO 20 OCT 2029

OY3: 21 OCT 2029 TO 20 OCT 2030

OY4: 21 OCT 2030 TO 20 OCT 2031

1.6.1 Transition: Transition-in/transition-out period

1.6.1.1 Transition-in period: Full performance start date is 01OCT2026. Transition-in performance is defined as 01OCT2026 TO 30SEP2027. During the transition-in period, the contractor shall prepare to meet all contract requirements and ensure incoming personnel are functionally trained and qualified on the full performance start date except cybersecurity requirements, which must be fully adhered during transition and full performance periods.

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

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

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

1.7 Administrative specifications

1.7.1 Place of performance: The work shall be performed at NMRTC San Diego, 34800 Bob

Wilson Drive San Diego, CA 92134.

1.7.2 Recognized Federal holidays:

New Year’s Day

Martin Luther King Jr.’s Birthday

President’s Day

Memorial Day

Juneteenth Day

Independence Day

Labor Day

Columbus Day

Veteran’s Day

Thanksgiving Day

Christmas Day

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

1.7.4 Emergency Services: N/A.

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

1.9 Other **Direct Costs (ODC)**: N/A

1.10 Quality

1.10.1 Quality Control (QC): The contractor shall develop and maintain an effective QC program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure nonrecurrence of defective services. The contractor's QC program is the means by which the work complies with stated requirements. After acceptance of the Quality Control Plan (QCP) the contractor shall receive the CO's acceptance in writing of any proposed change to his QC system. See Part 7, Technical Exhibit 1 - CDRL A001.

1.10.2 Quality assurance (QA): The government will evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan provides a systematic method for the Government to evaluate performance and to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

1.11 Contractor **personnel**

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

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

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

1.11.2.1 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>

1.11.2.2 The DHA’s contractor training instructions embedded at Part 7 Section 7.1.2.

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

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

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

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

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

1.11.5 Lock combinations: N/A

1.12 Key **personnel (Contractor)**: N/A

1.13 Data **rights**: N/A

1.14 Reporting

1.14.1 Contractor Manpower Reporting (CMR): RESERVED.

1.14.2 Non-Disclosure Agreement (NDA): N/A

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

1.15 Contractor Identification

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

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

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

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

1.16.1 FSO/Company's Security POC shall notify the DHA Personnel Security Office after being awarded a contract that requires access to a DoD system (If applicable, if not delete 1.16.1

and 1.16.2 and replace to 1.16 Reserved). Contractor personnel requiring access to the HA/DHA networks for performance of their tasks require a background investigation and the security awareness training. The contractor shall be prepared for this process as it could take two (2) or more weeks. The FSO/Security POC shall submit a Standard Form (SF) 85/86 to DHA's Personnel Security Office for a background investigation.

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

1.17 Personnel Security

1.17.1 The contractor shall comply with DoD 8570.01-M, "Information Assurance Workforce Improvement Program, CH4" November 10, 2015 as amended; 8500.01, "Cybersecurity", dated March 14, 2014; DoD Manual (DoDM) 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs" dated March 3, 2019, Department of Defense Instruction (DoDI) 6025.18 "HIPAA Privacy Rule Compliance in DoD Health Care Programs", dated March 13, 2019; and DoDM 5200.02 "Procedures for the DoD Personnel Security Program (PSP)," incorporation change 3, effective September 24, 2020. Contractor responsibilities for ensuring personnel security include, but are not limited to, meeting the following requirements:

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

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

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

PART 2

2.0 DEFINITIONS, ACRONYMS, AND APPLICABLE PUBLICATIONS/INSTRUCTIONS

2.1 Definitions:

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

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

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

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

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

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

2.2 Acronyms:

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

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

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

SRM	Sustainment, Restoration and Modernization
SRG	Security Requirements Guides
STIG	Security Technical Implementation Guides
TOS	Terms of Service
US	United States
UFC	Unified Facilities Criteria
VPN	Virtual Private Network
XML	Extensible Markup Language

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

PART 3
3.0 GOVERNMENT FURNISHED PROPERTY, EQUIPMENT, AND SERVICES

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

3.1 Services: The Government:

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

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

3.2 Facilities: The Government:

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

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

3.3 Utilities: The Government:

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

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

3.4 Equipment: The Government:

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

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

3.4.1 Procurement Integrated Enterprise (PIEE), GFP Module Application

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

Contracting Office Responsibilities:

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

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

Contractor Responsibilities:

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

The contractor shall report semi-annually 100% inventories, reconciliations, and final disposition of GFP provided by the government. Final invoices will not be paid pending GFP reconciliation. Contractors shall be aware of and ensure compliance with applicable FAR Part 45, DFARS 245 and 252.245, Defense Pricing and Contracting Policies, Procurement Integrated Enterprise Environment Standards, DHA Administrative Instruction 094 and DHA Guidance.

3.5 Materials: The Government:

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

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

PART 4
4.0 CONTRACTOR FURNISHED ITEMS AND SERVICES

4.1 Services: The Contractor:

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

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

4.2 General: The contractor shall furnish all supplies, equipment, facilities and services required to perform work listed under Section 5 of this PWS.

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

4.4 Materials: N/A

4.5 Equipment: N/A

4.6 Facilities: N/A

PART 5
5.0 SPECIFIC TASKS

5.1 Task Headings: The contractor shall provide all personnel, equipment, supplies, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Preventive Maintenance services for 2 government-owned Autotransfusion Unit as defined in this Performance Work Statement (PWS).

5.2 Special Qualifications:

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

PART 6

6.0 INFORMATION TECHNOLOGY & SECURITY

6.1 All work under this contract is N/A

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

6.2.1 TIER I: Critical sensitive position

OR 6.2.1 TIER II: Non-critical sensitive position.

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

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

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

6.4 Training

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.5.6 If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the CO or COR when requesting its recognition under this contract.

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

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

6.5.8 Cyber Incident Reporting Requirement

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

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

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

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

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

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

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

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

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

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

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

6.5.15. The contractor shall mitigate supply chain risk to the government by complying with DFARS 252.239-7018 and only utilizing unified capability equipment identified on the DODIN Unified Capabilities Approved Products List (<https://aplists.disa.mil/processAPList>), unless granted a waiver in accordance with DODI 8100.04, DOD Unified Capabilities (UC).

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

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

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

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

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

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

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

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

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

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

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

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

6.6.12 The contractor shall mitigate supply chain risk to the government by complying with DFARS 252.239-7018 and only utilizing unified capability equipment identified on the DODIN Unified Capabilities Approved Products List (<https://aplists.disa.mil/processAPList>), unless granted a waiver in accordance with DODI 8100.04, DOD Unified Capabilities (UC).

6.7. Facility Related Control Systems: The DHA’s Facilities Enterprise (FE) Program Management Office (PMO) establishes the processes for acquisition, installation and sustainment of FRCS in DHA Facilities. Requirements for cybersecurity of FRCS are developed and specified by the FHA FE FRCS PMO. The scope of PIT and Control Systems within the DoD includes building control systems such as Heating Ventilation and Air Conditioning, Utility Management Control System, Electronic Security Systems, Fire Alarm Systems, and other

assets. The application of IT cybersecurity strategies is migrating into PIT and Control Systems in response to emerging threats. The requirements within this scope apply to all versions of Design-Build (DB); Design-Bid-Build (DBB); and facilities Sustainment, Restoration and Modernization (SRM) projects as well as Initial Outfitting (IO) requirements activities.

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

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

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

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

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

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

of PP devices/systems will be through IO action entirely separate to the SRM, DBB, or DB contract, the same RMF-related activities are required. These activities shall be fully integrated into the project master schedule.

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

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

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

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

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

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

6.7.4.4 Contractors shall notify the assigned Government POC FRCS analyst of any updates/changes to the system and attain Government approval from the Military Treatment Facilities (MTFs) Change Control Board prior to installation. This should include operating system updates/patches; contractor application and database upgrades, updates, and patches; other software/firmware updates/patches; and addition/removal of components.

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

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

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

6.7.4.7.1 Minimum IPv6 capabilities include:

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

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

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

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

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

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

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

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

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

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

6.7.5.4 For all devices/systems requiring an ATO:

- (a) For SRM projects and IO requirements, the contractor shall not make any delivery and shall not receive payment until the Government POC has approved the self-assessment of the test/laboratory environment. The contractor must receive written confirmation from the CO that the system/device has successfully completed a self-assessment and that the contractor may proceed with delivery. Delivery may take place prior to this milestone only if written permission is provided by the CO.
- (b) For DBB and DB MILCON-funded FRCS, the contractor proceeds at his own risk if the contractor has not received Government approval that the system/device has successfully completed a self-assessment. Once the system/device has been installed, commissioning or acceptance testing shall not proceed until the Government POC, with contractor support and mitigation, has completed a successful self-assessment of the installation, and the Independent Verification & Validation (IV&V) has been scheduled (if required). An IV&V cannot be scheduled until all documentation requirements and technical requirements have been completed to the Government POC's satisfaction. Additionally,

all required POA&Ms must have been identified, and been appropriately mitigated to reduce the risk to the Government network and PHI/PII/For Official Use Only data housed within the system.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.7.8.3 The contractor shall maintain an ATO or APL approval on all equipment/product versions owned by the HA) and Services and originally purchased through the contractor's

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

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

6.7.9 Cybersecurity Requirements/Continuous Monitoring/Risk Management

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6.8. System Communications - RESERVED

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

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

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

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

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

6.10 Contractor Provided IT Infrastructure

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

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

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

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

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

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

6.11.2 The contractor shall submit the completed DD Form 2875 to the DHA IT Security for verification of Tier I or Tier II Designation. The DHA Personnel Security will verify that the contractor employee has the appropriate background investigation completed or a request for background investigation has been submitted to the Office of Personal Management (OPM). Acknowledgment from OPM that the request for a background investigation has been received and that an investigation has been scheduled will be verified by the DHA Personnel Security prior to access being approved.

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

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

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

6.12 MHS Systems Telecommunications

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

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

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

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

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

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

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

6.13 Establishment of Telecommunications

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

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

6.13.3 The DHA/MedCOI B2B Gateway Questionnaire (provided by DHA) identifies the required telecommunication infrastructure between the contractor and the MHS systems. This

includes all Wide Area Network, Local Area Network, VPN, Web DMZ, and B2B Gateway access requirements.

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

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

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

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

6.14 Contractors Located On Military Installations

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

6.14.2 These connections will be furnished by the Government.

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

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

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

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

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

The below attachment is designed to assist Government users in ensuring that the appropriate cyber and cloud references are include as necessary. Both this statement and the attachment are for Government use and should be deleted prior to publicizing the PWS to industry.)



DODIN Decision
Tree_160929.pptx

PART 7

7.0 ATTACHMENTS/TECHNICAL EXHIBIT LISTING

(Under this section list all attachments and technical exhibits that will be useful for the contractor to submit an appropriate proposal.)

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

7.1.1 Contractor CAC Request Process. *(If a more recent form is available, please replace the embedded version below.)*



DHA CAC Request
Process.pdf



DMDC TASS
Application.xlsx

7.1.2 DHA's contractor training instructions. *(Current form embedded from October 2021. If a more recent form is available, please replace the embedded version below.)*



DHA FY22 Annual
Training List_Oct 2021

7.1.3 DHA's new employee handbook. *(If applicable, if not delete entire 7.1.3 and the embedded document)*



DHA CAE (J-4) New
Employee Handboo

PART 7, ATTACHMENT 1 PERFORMANCE REQUIREMENTS SUMMARY

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

Performance Objective (The Service required—usually a shall statement from Part 5)	PWS Reference	Acceptable Quality Level (AQL) (This is the maximum error rate. It could possibly be “Zero deviation from standard”)	Method of Surveillance
Performance Requirements Summary (PRS) # 1. The contractor shall provide all personnel, equipment, supplies, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Preventive Maintenance and repair services for 2 government-owned Autotransfusion Units as defined in this Performance Work Statement (PWS).	PWS Part 5 Section 5.1.	95% of the units assigned must be completed in the month maintenance is due.	Completion surveillance will be administered by the Floor Supervisor (LPO) of the BIOMED shop. Any complaints will be received by the COR.
PRS # 2 (See example provided in PRS 1.)	(See example provided in PRS 1.)	(See example provided in PRS 1.)	(See example provided in PRS 1.)
PRS # 3 (See example provided in PRS 1.)	(See example provided in PRS 1.)	(See example provided in PRS 1.)	(See example provided in PRS 1.)
PRS # 4 (See example provided in PRS 1.)	(See example provided in PRS 1.)	(See example provided in PRS 1.)	(See example provided in PRS 1.)

The following listing provides various types of Surveillance as examples to select from and should not be included on the final document:

Random Sampling: *Appropriate for frequently recurring tasks. Evaluate randomly selected samples of the lot to determine the acceptability of the entire lot.*

Random Inspection Guide, Method of surveillance, Lot size, Sample size, Performance requirement, Sampling procedure, Inspection procedure.

100 Percent Inspection: *Appropriate for tasks that occur infrequently. Inspect and evaluate performance each time task is performed.*

Periodic Surveillance: *Evaluation of samples selected on other than 100% or statistically random basis. (i.e., monthly, quarterly, semi-annually etc.)*

Validated Customer Complaint: *Complaints must be validated.*

NOTE: YOU MAY ALSO IDENTIFY ANY SURVEILLANCE METHOD USED IN THE COMMERCIAL MARKET TO SURVEY THE REQUIRED SERVICE. (THIS WILL BE DISCOVERED WHEN MARKET RESEARCH IS CONDUCTED).

7.2 Other Attachments

Attachment 2, Deliverable Schedule Table (Paragraph 6.5.2.1.1)



Attachment
2-Deliverable Schedul

Attachment 3, Cybersecurity Regulations and Guidance (Paragraph 6.7.2.3)



Attachment
3-Cybersecurity Regu

Attachment 4, FRCS Responsibility Matrix (Paragraph 6.7.5.3)



Attachment 4-FRCS
Responsibility Matrix,

Attachment 5, Risk Assessment Timeframes (Paragraph 6.7.7)



Attachment 5-Risk
Assessment Timefram

PART 7, ATTACHMENT 6
ESTIMATED WORKLOAD DATA

(This technical exhibit lists the historical estimated workload data, i.e., the estimated hours previously performed under the PWS by labor category. This workload data should be used to prepare the IGCE, if available. Note: Based on the PWS, historical workload data can be provided in other formats, i.e., the volume of task orders issued over a five year period, the number of users by locations requiring IT Support, etc. If hours are used, then the estimated quantity for each labor category should be the annual (e.g. 12 month) quantity.)

ITEM	NAME	ESTIMATED QUANTITY
1	[Insert the Labor Category, i.e., Network Specialist, etc.]	[Insert the number of hours, i.e., 200 Hours, etc.]
2	[Continue to insert the Labor Categories, using example provided above.]	[Same as above.]
3	[Same as above.]	[Same as above.]
4	[Same as above.]	[Same as above.]
5	[Same as above.]	[Same as above.]

PART 7, TECHNICAL EXHIBIT 1 DELIVERABLES SCHEDULE

(This technical exhibit lists any reports or documentation that is required as a deliverable to include the frequency, # of copies, medium/format and who/where it is to be submitted. A deliverable is anything that can be physically delivered but may include non-physical things such as meeting minutes. Note: All PWS deliverables should be included in this exhibit.)

<u>Deliverable</u>	<u>Frequency</u>	<u>Medium/Format</u>	<u>Submit To</u>	<u>Applicable to:</u>
CDRL A001 – Quality Control Plan  CDRL 1 Quality Plan	Within 30 days of task order award	Contractors discretion	CDRL A001 to CO	All, See PWS 1.10.1
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.
[Additional CDRLs may be added when required or beneficial to the contract; delete entire row if not adding additional CDRLs.]	[Insert how often it is to be provided, i.e., by the 5 th of every month, within 30 days of contract award, etc.]	[Insert the medium/format that the deliverable is to be provided in, i.e., paper (hard copy), CD in MS Word, DVD, Briefing Slides on CD, Excel Spreadsheet, etc.]	[List office/function name and contact information (if applicable for delivery.)]	[Added PWS reference.]
[Same as above; delete entire row if not adding additional CDRLs]	[Same as above.]	[Same as above.]	[Same as above.]	[Same as above.]