SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS
OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE 1 of 142
1000247071	

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
			SPE2D1-27-R-0001	2026 OCT 15

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (*No Collect calls*)	8. OFFER DUE DATE/ LOCAL TIME
	Zahkiyah Taylor DZA0003	Phone: 4457377362	2033 OCT 14 03:00 PM

9. ISSUED BY — CODE SPE2D1

DLA TROOP SUPPORT
MEDICAL SUPPLY CHAIN FSD
700 ROBBINS AVENUE
PHILADELPHIA PA 19111
USA

10. THIS ACQUISITION IS
- ☒ UNRESTRICTED OR ☐ SET ASIDE: _____ % FOR:
- ☐ SMALL BUSINESS
- ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- ☐ HUBZONE SMALL BUSINESS
- ☐ EDWOSB — NAICS: 334510
- ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- ☐ 8 (A) — SIZE STANDARD: 1,250

11. DELIVERYFOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
☐ SEE SCHEDULE		☐	RFQ ☐ IFB ☐ RFP ☒

15. DELIVER TO — CODE

SEE SCHEDULE

16. ADMINISTERED BY — CODE

17a. CONTRACTOR/ OFFEROR — CODE — FACILITY CODE

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY — CODE

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

☐ 18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED — ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	See Schedule *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*

☒ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☒ ARE ☐ ARE NOT ATTACHED

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

☐ 29. AWARD OF CONTRACT: REF._____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR		31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*	
30b. NAME AND TITLE OF SIGNER *(Type or Print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or Print)*	31c. DATE SIGNED

Contents

Continuation of Blocks from SF 1449 ..... **3**
1. Block 8 3
2. Block 9 3
3. Block 17a 3
4. Block 17b 3
5. Blocks 19-24 3
Caution Notices **5**
Caution Notice 1 – Proposal Checklist 5
Caution Notice 2 – Contractor Code of Business Ethics 5
Caution Notice 3 – Offeror Exceptions to Terms and Conditions 6
Caution Notice 4 – FAR and DFARS Overhaul 6
Caution Notice 5 – Significant Cybersecurity Provisions and Clauses 7
Section B – Supplies or Services and Prices/Costs **7**
Section C - Description/Specifications/Requirements **8**
Statement of Work 8
SOW - Cardiology 10
SOW - Dental 16
SOW - Dermatology 20
SOW - Endoscopy 24
SOW - Nuclear Medicine 28
SOW - OB-GYN 31
SOW - Oncology 35
SOW - Ophthalmology 39
SOW - Pathology 43
SOW - POCUS 47
SOW - Radiology 51
SOW - Sleep Lab 54
SOW - Veterinary 58
SOW - Vendor Neutral Archive 62
SOW Appendix 1 – DICOM Requirements 65
SOW Appendix 2 – Contract Data Requirements List (CDRL) 67
SOW Appendix 3 – Installation, Extended Installation, Interfaces/Integration 76
SOW Appendix 4 – Inspection and Acceptance 80
SOW Appendix 5 – Training, System Reliability, and Maintenance 87
SOW Appendix 6 – Cybersecurity 94
SOW Appendix 7 – DIN-PACS Lifecycle System Support and Software Requirements 101
Section G – Contract Administration Data **104**

Section H – Special Contract Requirements **105**
Section I - Contract Clauses **110**
Section J - List of Attachments **126**
Section K – Representations, Certification, and Other Statements of Offerors **126**
Section L – Instructions, Conditions, and Notices to Offerors or Respondents **132**
Section M – Evaluation Factors for Award **140**
VA Issued Delivery Orders **141**

Continuation of Blocks from SF 1449

NOTE: The terms Vendor, Contractor, and Offeror are used in this document interchangeably.

1. Block 8 Offer Due Date/Local Time: 3:00PM Philadelphia, PA, local time, October 14, 2033. This is a standing solicitation, see details in 52.212-1.

2. Block 9 Issued By: Proposals must be submitted through the Procurement Integrated Enterprise Environment (PIEE) at https://piee.eb.mil/. No other means are authorized. See details following this continuation of blocks. Questions concerning the solicitation, and notices of proposal submission, revision, or withdrawal shall be emailed to Christine.Welker@dla.mil and Zahkiyah.Taylor@dla.mil.

3. Block 17a Contractor/Offeror:

Offeror's assigned Unique Entity Identifier (UEI) Number: _____.

Offeror's assigned Contractor and Government Entity (CAGE) Code: _____.

(See details following this continuation of blocks)

4. Block 17b Remittance Address**:** (if different from Contractor/Offeror address in block 17a of the SF 1449.)

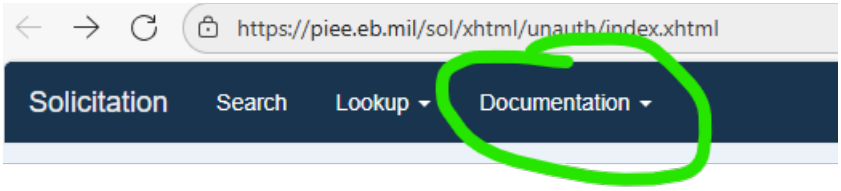
_____
_____
_____

5. Blocks 19-24 Item No., Schedule of Supplies/Services, Quantity, Unit:

See Section B.

(End Continuation of Blocks from SF 1449)

PIEE, SAM, CAGE, and UEI. PIEE (https://piee.eb.mil/) is a DoD web-based application that provides the capability to search for, view, and submit secure proposal submissions. Follow the website's documentation in the Solicitation Module at https://cac.piee.eb.mil/sol/xhtml/unauth/index.xhtml regarding the Proposal Manager to register and submit and offer.



Offerors are advised to read the Proposal Manager documents in their entirety before registering, to ensure any initial steps have been completed, such as registering in SAM.gov and obtaining a Commercial and Government Entity (CAGE) code. If you do not have a CAGE code, one will be assigned to you when you complete the SAM registration. SAM registration will also provide you with a Unique Entity Identifier (UEI) number. SAM registration is separately required for award and duration of performance. For more information, visit https://sam.gov/entity-registration and https://www.dla.mil/Vendor-Information-Hub/Table-of-Contents/Details/Article/3606127/registration-renewal-and-cage-creation-in-system-for-award-management-sam/.

Caution Notices

These Caution Notices are part of the solicitation and any resultant contract.

Caution Notice 1 – Proposal Checklist

Below is a general checklist of the information offerors shall submit with their offer under this Request for Proposal. Please review the checklist below to help ensure proposal completeness. Offerors shall answer all questions listed below and provide all the information requested as part of their proposal. Proposals that are found to be missing required information may be rejected without further evaluation.

Did you provide a completed Solicitation Form, signed and dated, with Completed Continuation Pages (provisions and clauses in this document contain fill-ins)?

☐ **YES** ☐ **NO**

Did you provide and complete all required submission attachments, including Attachment A – Vendor Price Book, Attachment B – Discount & Pricing Information, Attachment C – Offeror Exceptions to Terms and Conditions (if applicable), and Attachment D – Statement of Work Responses?

☐ **YES** ☐ **NO**

Did you provide all supporting documentation requested in the Attachments?

☐ **YES** ☐ **NO**

Did you provide written information to address the evaluation factors Product Offering, Experience, and Past Performance (Experience and Past Performance are not required with initial proposal if the offeror is eligible for Streamlined Offering)?

☐ **YES** ☐ **NO**

Did you provide a copy of your current Commercial Catalog with your proposal?

☐ **YES** ☐ **NO** ☐ **N/A**

Did you provide a copy of your current Federal Supply Schedule contract with your proposal?

☐ **YES** ☐ **NO** ☐ **N/A**

If your company is not a small business for NAICS Code 334510, did you include your Small Business Subcontracting Plan (reference 52.219-9 Alternate II and 252.219-7996)?

☐ **YES** ☐ **NO**

Caution Notice 2 – Contractor Code of Business Ethics

FAR Part 3.1002(a) requires all government contractors to conduct themselves with the highest degree of integrity and honesty. Contractors should have a written code of business ethics and conduct within thirty days of award. To promote compliance with such code of business ethics and conduct, contractors should have an employee business ethics and compliance training program that facilitates timely discovery and disclosure of improper conduct in connection with government contracts and ensures corrective measures are promptly instituted and carried out. A contractor may be suspended and/or debarred for knowing failure by a principal to timely disclose to the government, in connection with the award, performance, or closeout of a government contract performed by the contractor or a subcontract awarded there

under, credible evidence of a violation of federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the United States Code (U.S.C.) or a violation of the False Claims Act. (31 U.S.C. §§ 3729-3733)

If this solicitation or contract includes FAR clause 52.203-13 - CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT; the contractor shall comply with the terms of the clause and have a written code of business ethics and conduct; exercise due diligence to prevent and detect criminal conduct; promote ethical conduct and a commitment to compliance with the law within their organization; and timely report any violations of federal criminal law involving fraud, conflict of interest, bribery or gratuity violations found in title 18 of the United States Code or any violations of the False Claims Act. (31 U.S.C. §§ 3729-3733). When FAR 52.203-13 is included in the contract, contractors must provide a copy of its written code of business ethics and conduct to the contracting officer upon request by the contracting officer.

Caution Notice 3 – Offeror Exceptions to Terms and Conditions

By submitting an offer, the offeror understands and agrees to comply with the requirements of all provisions and clauses. Further, notwithstanding any exception noted within the body of the solicitation, attachments, or proposal, by submitting an offer the offeror agrees that it has not taken exceptions to any term or condition of this solicitation unless explicitly identified by the offeror on Attachment C - Offeror Exceptions to Terms and Conditions. Offeror exceptions to Terms and Conditions on Attachment C may lead to amendment of the Solicitation, clarifications or negotiations with the offeror, or rejection of the offer, in the sole discretion of the Contracting Officer.

Caution Notice 4 – FAR and DFARS Overhaul

This procurement is using the procedures of Revolutionary FAR Overhaul (RFO) 12.201-2.

In Fiscal Year 2026, the Department of War (DoW) issued RFO class deviations to the FAR and DFARS codified text. The text of the deviations to the DFARS are found at Defense Pricing, Contracting, and Acquisition Policy (DPCAP) website, https://www.acq.osd.mil/dpap/dars/dfars_far_overhaul_class_deviations.html, with deviations to the FAR incorporated by reference, citing https://www.acquisition.gov/far-overhaul. These deviated sections contain the provisions and clauses governing this solicitation and resulting contracts.

Provisions and Clauses from the FAR Overhaul will be denoted by FAR with the appropriate DoW 2026 deviation number that adopted Overhaul Part 52. Deviations prior to 2026 may still have effect, which are also indicated when applicable. Provisions and Clauses from the DFARS Overhaul are denoted with just the DoW deviation number, as text of those provisions and clauses are included at the end of each deviation on the DPCAP website.

In Fiscal Year 2026, the Department of Veterans Affairs (VA) issued RFO class deviations to the FAR and VA Acquisition Regulations (VAAR) codified text. The text of the deviations to the VAAR are found at https://www.va.gov/oal/business/pps/deviations.asp, with deviations to the FAR incorporated by reference, citing https://www.acquisition.gov/far-overhaul. These deviated sections contain the provisions and clauses governing this solicitation and resulting contracts.

VAAR Provisions and Clauses from the FAR Overhaul will be denoted by FAR with the text “VAAR Deviation” along with the effective date of the deviation that adopted the Overhaul Part.

The pre-RFO full text of the VAAR can be found at https://www.va.gov/oal/library/vaar/index.asp.

Caution Notice 5 – Significant Cybersecurity Provisions and Clauses

In addition to changes to DHA, VA, and site-specific cybersecurity requirements detailed in their documents, the following (referenced here for informational purposes) are included in this solicitation among others that may be related to cybersecurity:

52.240-93 Basic Safeguarding of Covered Contractor Information Systems
252.204-7008 Compliance with Safeguarding Covered Defense Information Controls
252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting
252.239-7017 Notice of Supply Chain Risk
252.239-7018 Supply Chain Risk
852.204-70 Personal Identity Verification of Contractor Personnel
852.204-71 Information and Information Systems Security

Section B – Supplies or Services and Prices/Costs

DLA Troop Support and the Veterans Administration (VA) National Acquisition Center (NAC) are requesting offers for commercial products and components in the following Digital Imaging Network - Picture Archiving and Communications Systems (DIN-PACS) specialties:

(a) Cardiology
(b) Dental
(c) Dermatology
(d) Endoscopy
(e) Nuclear Medicine
(f) OB/GYN
(g) Oncology
(h) Ophthalmology
(i) Pathology
(j) Point of Care Ultrasound (POCUS)
(k) Radiology
(l) Sleep Lab
(m) Veterinary
(n) Point of Care Ultrasound (POCUS)
(o) Vendor Neutral Archive (VNA)

See the Statement of Work and its Appendices for minimum product requirements, and requirements for documentation, training, maintenance, and incidental services that are to be included with the DIN-PACS offering. Incidental services are any site-specific work or non-contract items, including professional services (e.g. onsite project management, system administration) and extended installation, needed to provide and deliver to the Government a fully operational turnkey DIN-PACS product.

Vendors may offer multiple types of DIN-PACS solutions (e.g., Radiology, Cardiology, etc.) within a single proposal or add solutions through modification after contract award has been received for at least one solution.

Unless otherwise authorized, all items supplied shall be new, original manufacturer items. They shall not consist of any reconditioned, rebuilt, or remanufactured items. The Contractor shall be an Original Equipment Manufacturer (OEM), authorized dealer, authorized distributor, or authorized reseller for the proposed equipment or system, as verified by an authorization letter or other documentation issued by the OEM. All software licensing, warranties, and services associated with the equipment or system shall be provided in accordance with the OEM's terms and conditions.

The offered schedules of supplies, list prices, offered discounts from list prices, and the resulting net prices shall be provided on Attachment A – Vendor Price Book (See Instructions for Attachment A in Solicitation Provisions). Price adjustments during contract performance are governed by the Economic Price Adjustment (EPA) Clause TS 16-08 in this solicitation. Discounts from list prices may not be reduced (but may be increased by the Contractor) during the life of a resulting contract. Prices offered for each item shall include the price of all necessary components and accessories, such as adapting parts, when the subject item is installed with other offered items, or existing on-hand compatible items.

Unpriced components that are necessary to the configuration or operation of a system and are included in the price of the system, but are not separately priced in the Vendor Price Book, may be included as individual line items on a delivery order without being listed in the Vendor Price Book. Such components shall be identified in the vendor's offer and noted as a non-Price Book item. Unpriced components included in delivery orders shall be determined otherwise technically acceptable, including meeting all regulatory approvals (e.g. Food and Drug Administration (FDA) 510(k) Clearance), and be within the scope of this solicitation.

Under certain circumstances vendors are unable to set a fixed price for items such as incidental/professional services or third-party items at time of basic contract award. See Price Reasonableness Determinations in this solicitation for items not pre-priced under contract, in Paragraph 5 of the additional instructions to offerors in Section L. A separate part number shall be used for each separately identifiable service/item, and each service/item shall meet. These services/items shall be technically acceptable, including meeting all regulatory approvals (e.g. FDA 510(k) Clearance), be U.S. made, qualifying country or designated country end products and be within the scope of this solicitation.

Delivery locations will be established at the delivery order level. Delivery locations are in the contiguous United States (CONUS), which includes the 48 contiguous States and the District of Columbia, and areas outside of the contiguous United States (OCONUS). Vendors shall support all CONUS locations plus Alaska, Hawaii, and U.S. Territories. Contract pricing shall be provided on Attachment A on a FOB Destination basis for all CONUS locations. At the delivery order level, different FOB Destination pricing may be provided for Alaska, Hawaii, the US Territories, and other OCONUS locations (e.g. Europe and Pacific), if consistent with commercial practice and can be determined as fair and reasonable by the Contracting Officer. Acceptable price support information shall be provided by the vendor to substantiate the different pricing during the delivery order award process.

Delivery timelines will be determined at the delivery order level.

Section C - Description/Specifications/Requirements

Statement of Work

DLA Troop Support and the VA National Acquisition Center (VA NAC) are requesting offers for DIN-PACS systems and components that meet the minimum essential characteristics defined herein. Requirements for Contract Data Requirements List (CDRL) documentation, training, maintenance service, and incidental services related to the supply of the DIN-PACS are to be included with the offering. Incidental services include all professional, technical, project-management, and site-specific activities required to deliver a fully operational DIN-PACS solution.

Unless otherwise noted, the Government is soliciting for strictly commercial material in accordance with the FAR Part 12 "Acquisition of Commercial Products and Commercial Services."

Unless otherwise authorized, all items supplied shall be new, original manufacturer items. They shall not consist of any reconditioned, rebuilt, or remanufactured items.

The DIN-PACS configuration may be offered as either a fully integrated system or as individual components within a modular and/or deconstructed architecture, provided all components operate reliably and meet all functional, interoperability, security, and performance requirements. All images and associated metadata shall be stored in a non-proprietary, open standard DICOM format, throughout their lifecycle, including within all PACS and Vendor Neutral Archive systems. To ensure enterprise-wide interoperability, all systems, components, and viewers shall natively support open, standards-based Application Programming Interfaces (APIs)—including DICOM, DICOMweb services and HL7 for secure, bi-directional data exchange, cloud streaming, and integration across all specialties and third-party systems without requiring proprietary middleware.

All DIN-PACS products offered for a specialty shall meet the minimum essential characteristics for the specialty stated herein. Additionally, each offered system shall meet the requirements of each Appendix. The vendor shall provide a full range of medical grade hardware (e.g., workstations and diagnostic displays) that meet all applicable federal, clinical, and technical standards for each clinical specialty. Additionally, hardware must comply with Occupational Safety and Health Agency (OSHA) requirements, Health Insurance Portability and Accountability Act (HIPAA) protections for systems accessing Protected Health Information (PHI), Centers for Disease Control and Prevention (CDC) Infection Control guidelines for operatory based units, the DICOM Standard (per https://www.dicomstandard.org/), FDA requirements, and all applicable Trade Agreements Act (TAA) regulations. Deployments may occur on-premises, within a government-managed or controlled cloud environment, or through any combination of these options, all of which are within scope.

Systems may include items categorized as “Components” where they use a part number/price structure that lists separately components that make up the end item. System components allow addition of minor components to the contract that are not manufactured in countries cited in the Trade Agreement Act (TAA) but are components of a higher-level end item that is fully compliant with DFARS 252.225-7021 Trade Agreements (FEB 2024). All the following conditions must be met by a Component in order to be allowable under the contract and to comply with TAA regulations:

(1.) The item must be a minor component of a higher-level end item that is TAA compliant.

(2.) The component(s) shall never be purchased individually and can only be ordered as part of the higher-level end item that is fully TAA compliant.

(3.) The vendor shall provide all information typically provided for product addition requests for regular end items; including price, country of origin, product description, etc.; along with additional information specifying the system(s) that they are part of on the indicated areas of the price book. Applying the Country of Origin from a higher-level end item is not acceptable.

(4.) The item(s) shall be identified in the price book by choosing “COMPONENT” in the product category field.

(5.) The vendor certifies that all end items that are delivered to the Government under this contract are in full compliance with DFARS 252.225-7021 Trade Agreements (FEB 2024).

When required, the Contractor shall make available capabilities to support migration from current Government imaging platforms to the offered DIN-PACS solution. All migration efforts shall be included (if required) as part of system delivery and executed to facilitate a seamless transition with minimal impact on clinical operations. The migration solution shall ensure data integrity, completeness, accuracy, and traceability throughout the entire migration lifecycle. The migration process shall support DICOM-compliant imaging data, non-DICOM imaging files, and associated metadata, and shall include automated and manual validation to ensure no loss of data, preservation of image quality, and accurate patient to image association.

Offers not meeting these requirements will be deemed technically unacceptable and will not be considered for contract award.

Statement of Work 8
SOW - Cardiology 10
SOW - Dental 16
SOW - Dermatology 20
SOW - Endoscopy 24
SOW - Nuclear Medicine 28
SOW - OB-GYN 31
SOW - Oncology 35
SOW - Ophthalmology 39
SOW - Pathology 43
SOW - POCUS 47
SOW - Radiology 51
SOW - Sleep Lab 54
SOW - Veterinary 58
SOW - Vendor Neutral Archive 62

SOW Appendix 1 – DICOM Requirements 65
SOW Appendix 2 – Contract Data Requirements List (CDRL) 67
SOW Appendix 3 – Installation, Extended Installation, Interfaces/Integration 76
SOW Appendix 4 – Inspection and Acceptance 80
SOW Appendix 5 – Training, System Reliability, and Maintenance 87
SOW Appendix 6 – Cybersecurity 94
SOW Appendix 7 – DIN-PACS Lifecycle System Support and Software Requirements 101

SOW - Cardiology

The vendor shall provide a comprehensive Cardiology Picture Archiving and Communication System (Cardiology PACS) designed to support real-time image acquisition, review, reporting, and long-term management of cardiovascular imaging and diagnostic data. The Cardiology PACS shall deliver an integrated platform capable of handling multimodality cardiology studies, including but not limited to echocardiography, cardiac catheterization, Electrocardiogram (ECG) management, hemodynamic monitoring systems, vascular imaging, nuclear cardiology, cardiac Computed Tomography (CT), and cardiac Magnetic Resonance Imaging (MRI). The Cardiology PACS shall include all required hardware components, software applications, licensing, diagnostic and clinical workstations/viewers, structured reporting tools, and associated support services necessary to provide a fully integrated cardiovascular imaging and information management environment optimized for cardiology workflows.

CARD 1. General System Requirements

CARD 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

CARD 1.2.

The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

CARD 1.3. Implements high-availability architecture with redundancy across servers, storage, and network components.

CARD 1.4. Provides secure, flexible storage architecture supporting SAN (Storage Area Network), NAS (Network Attached Storage), and object storage, ensuring preservation, rapid retrieval, and efficient management.

CARD 1.5. Provides scalable infrastructure (if offered) capable of supporting large cardiology imaging volumes and multimodality data.

CARD 2. Imaging Modality Support Requirements

CARD 2.1. Receives and archives images from echocardiography, angiography, cardiac MRI, cardiac CT, nuclear cardiology, and Doppler ultrasound.

CARD 2.2. Supports advanced visualization including 3D reconstruction, strain analysis, perfusion maps, and coronary CT angiography.

CARD 2.3. Ingests real time imaging data from Cath lab and hemodynamic monitoring systems.

CARD 2.4. Integrates seamlessly with ECG carts, resting ECG systems, stress ECG systems, Holter monitors and other cardiac monitoring devices to ensure unified acquisition, ingestion, and review.

CARD 2.5. Supports side by side comparison of current and prior studies for longitudinal tracking.

CARD 2.6. Provide quantitative analysis tools including LV function, wall motion, and perfusion defects.

CARD 2.7. Supports fusion imaging (PET/CT, SPECT/CT, CT/MRI fusion).

CARD 3. Reporting, Workflow, and Tools

CARD 3.1. Supports metadata-based search and retrieval by patient ID, modality, study type, procedure type, waveform type, or clinical indication.

CARD 3.2. Supports configurable retention, deletion, and archival policies for all cardiology data including imaging, waveforms, ECG, and Holter studies. and enables administrators to automate or manually execute record removal based on study type, data age, regulatory mandates, or organizational retention policies.

CARD 3.3. Provides a centralized administrative console for configuration, monitoring, user management, and cardiology specific workflow settings.

CARD 3.4. Supports automated study reconciliation for mismatched, incomplete, or duplicate cardiology study metadata.

CARD 3.5. Provides administrative tools for storage monitoring, capacity forecasting, performance metrics, and cardiology specific utilization reporting.

CARD 3.6. Provides a consolidated, real-time worklist that includes all cardiology exam types (ECG, Holter, stress, ambulatory monitoring, etc.) and supports filtering by location, provider, modality, and status.

CARD 3.7. Supports role-based workflows for cardiologists, radiologists (if applicable), cardiac technicians, and support staff, including configurable task routing, reading queues, and approval workflows.

CARD 3.8. Supports visual serial comparison of ECGs across all supported cart models and acquisition devices, including waveform overlay, side by side comparison, and automated measurement comparison.

CARD 3.9. Provides comprehensive, customizable structured reporting tools for all major cardiology subspecialties, supporting automated measurements, standardized templates, advanced annotation, and full physician review workflows.

CARD 3.10. Supports ingestion of Holter and ambulatory ECG data from multiple vendors and device types.

CARD 3.11. Stores ECG and waveform data using DICOM Waveform Storage or other standards-based formats to ensure long term accessibility and interoperability.

CARD 3.12. Supports high-performance ECG viewing, ECG waveforms and Holter summaries.

CARD 3.13. Supports Configurable Templates & Workflow:

(a) Supports configurable, structured reporting templates across cardiology subspecialties, offering customizable templates for areas such as Echocardiography, Cardiac Catheterization, Nuclear Cardiology, ECG, and Holter and Ambulatory ECG monitoring.;

(b) Supports physician overread, approval, and signature workflows and

(c) Enables configurable reporting fields, macros, and structured data elements.

CARD 3.14. Provides advanced annotation and measurement tools including chamber dimensions, ejection fraction, valve gradients, Lesion quantification, waveform annotation and comparison.

CARD 3.15. Enables workflow management including study assignment, status tracking, and turnaround monitoring.

CARD 3.16. Integrates with dictation, voice recognition, and other Natural Language Processing (NLP) i.e. AI platforms.

CARD 3.17. Provides collaboration tools for multidisciplinary heart team reviews and case conferences.

CARD 4. DICOM & Imaging Standards Requirements

CARD 4.1. Maintains full DICOM compliance for all cardiology relevant SOP Classes, Information Object Definitions (IODs), and service classes, including those used by Echocardiography, Cardiac CT, Cardiac MRI, Nuclear Cardiology, and Hemodynamic systems.

CARD 4.2. Supports DICOM-approved lossless and lossy compression methods optimized for large cardiology datasets, including cine loops, multi-phase CT, and MRI series, and provides configurable compression rules based on modality, study type, or archive tier.

CARD 4.3. Complies with DICOM Modality Worklist (MWL) for all cardiology modalities:

(1) DICOM Query/Retrieve (C FIND, C MOVE, C GET).
(2) DICOM Storage (C STORE).
(3) DICOM Modality Performed Procedure Step (MPPS).
(4) DICOM Presentation States.
(5) DICOM Hanging Protocols.
(6) DICOM Encapsulation (e.g., ECG waveforms, PDF reports).

CARD 4.4. Supports DICOM MPPS to track study completion and acquisition details.

CARD 4.5. Provides data integrity protocols to ensure end to end validation of DICOM objects (including SOP Class checks and UID consistency); redundant storage and replication across primary and secondary archives; and automated integrity monitoring with alerts for corruption or missing frames.

CARD 4.6. Supports HL7 messages to include:

(1) ADT
(2) ORM
(3) ORU
(4) SIU

CARD 4.7. Supports the following IHE Profiles:

(1) Scheduled Workflow (SWF).
(2) Patient Information Reconciliation (PIR).
(3) Consistent Presentation of Images (CPI).
(4) Evidence Documents (ED).
(5) Key Image Note (KIN).
(6) Audit Trail and Node Authentication (ATNA).

CARD 4.8. Supports:

(1) Automatic prefetching of prior cardiology studies.
(2) Worklist driven reading workflow.
(3) Multi-modality cardiology images and waveforms.
(4) Consistent hanging protocols across users.
(5) Advanced visualization (3D/4D echo, strain analysis, fusion imaging).
(6) Reporting integration (voice recognition, structured cardiology templates).
(7) DFT split billing interface.

CARD 4.9. Supports ingestion, storage, and query of cardiology specific modality attributes.

CARD 4.10. Complies with all cardiology specific regulatory standards (i.e. Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), FDA, etc.).

CARD 4.11. Complies with DICOM Structured Reporting standards and supports all relevant cardiology SR object types, including: echocardiography SR, cardiac catheterization SR, ECG waveform SR, Key Object Selection (KOS), and measurement/annotation SR templates.

CARD 4.12. Supports ad hoc queries with search criteria based on values or ranges for cardiology specific data elements, supporting logical operators and sortable results.

CARD 5. Security and Compliance Requirements

CARD 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

CARD 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

CARD 5.3 Encrypts all protected health information Protected Health Information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

CARD 5.4 Complies with all applicable privacy and security regulations, including: HIPAA; GDPR for facilities handling European Union (EU) patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools

CARD 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

CARD 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

CARD 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

CARD 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

CARD 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

CARD 6. Interoperability Standards

CARD 6.1. Supports standards-based interoperability required for exchanging orders, results, waveforms, images, and clinical data with enterprise Electronic Health Record (EHR) systems.

CARD 6.2. Supports all relevant IHE Cardiology integration profiles and DICOM workflow services—including Modality Worklist (MWL), Modality Performed Procedure Step (MPPS), and Storage Commitment—to ensure accurate, automated, and consistent workflow interoperability across cardiology imaging and reporting systems.

CARD 6.3. Provides Conformance Statements covering all DICOM functions of the proposed Cardiology PACS solution.

CARD 6.4. Supports HL7 v2.x messaging, including ORM, ORU, ADT, and SIU transactions, to enable standards-based order, results, and scheduling interoperability with enterprise EHR systems.

CARD 6.5. Supports SCP-ECG or equivalent standards for ECG waveform exchange, as well as DICOM Waveform Storage for ECG, hemodynamic, and stress test data.

CARD 7. System Performance and Availability Requirements

CARD 7.1 Provides rapid acquisition, rendering, and playback of cardiac imaging modalities (e.g. echocardiography loops, Cath lab cine runs, and stress echo sequences), with low latency and full frame rate performance.

CARD 7.2 Supports scalable performance to accommodate increasing volumes of echo studies, Cath lab procedures, ECG waveforms, hemodynamic data, and concurrent cardiologist review sessions without degradation in responsiveness.

CARD 7.3 Enables efficient access to archived cardiology studies, including echo loops, cine angiograms, ECGs, and hemodynamic reports, to support diagnostic evaluation and intra-procedural workflows.

CARD 7.4 Optimizes performance across cardiology-specific environments (e.g. Cath lab control rooms, echo lab workstations, mobile rounding devices, tablets, and telehealth platforms) ensuring consistent playback quality and responsiveness.

CARD 7.5 Includes performance monitoring dashboards and analytics tailored to cardiology workflows, providing visibility into system health, frame-rate performance, cine playback responsiveness, ECG waveform rendering, and usage patterns across modalities.

CARD 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention, without loss of data integrity, and without interrupting active cardiology workflows such as Cath lab procedures or live echo acquisition.

CARD 7.7 Implements a high-availability architecture and disaster recovery design that ensures uninterrupted cardiology operations (e.g. Cath lab, echo lab, telemetry, and ECG review) across outpatient clinics, hospitals, and telehealth environments, delivering a minimum of 99.9% system uptime.

CARD 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting cardiology imaging, waveform processing, or reporting. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

CARD 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to cardiology workflows, including echo playback, cine rendering, ECG waveform access, and hemodynamic data retrieval. All test results shall be logged and made available for audit and compliance review.

CARD 8. Augmented Intelligence (AI) Requirements

CARD 8.1. Provides AI-assisted detection and triage tools for cardiology use cases, including arrhythmia detection, ischemia or ST-segment abnormalities, wall-motion abnormalities, valvular disease assessment, coronary calcium scoring, and identification of perfusion defects.

CARD 8.2. Supports automated measurements including lesion size, volumetrics, and perfusion metrics.

CARD 8.3. Provides real-time acquisition guidance and quality feedback.

CARD 8.4. Integrates AI outputs into structured reporting workflows.

CARD 8.5. Provides predictive analytics for risk stratification and treatment planning.

CARD 8.6. Ensures explainable AI outputs with confidence scores and overlays.

CARD 8.7. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

CARD 8.8. Validation of AI algorithms against diverse datasets to ensure accuracy across patient demographics.

SOW - Dental

Vendor's products shall provide a comprehensive Dental Picture Archiving and Communication System (PACS) designed to support a wide range of digital dental imaging workflows. The Dental PACS shall include all necessary components—software, licensing, and incidental support services, to deliver a fully integrated data and imaging management platform.

DENT 1. General System Requirements.

DENT 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

DENT 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

DENT 1.3. Utilizes vendor-neutral architecture and fully complies with interoperability standards, including DICOM (for waveform and video data), HL7 (for clinical messaging), and FHIR (for RESTful data exchange), DoD & VA EHR platforms, and Enterprise archives.

DENT 1.4. Provides scalable infrastructure to accommodate increasing volumes of dental imaging studies, expanded clinical service offerings, and multi-site deployments across networked dental facilities.

DENT 1.5. Integrates with dental diagnostic tools to support quantification, segmentation, and assessment of treatment response across imaging modalities such as panoramic X-rays, cone-beam CT, and intraoral scans.

DENT 1.6. Provides flexible and secure storage infrastructure with support for lossless image compression and advanced metadata indexing (e.g., tooth number, arch, modality, acquisition parameters) to enable efficient retrieval, comparison, and analysis of dental imaging studies.

DENT 2. Imaging Modality Support Requirements

DENT 2.1. Securely receives and archives high-resolution dental imaging studies, including intraoral X-rays, panoramic radiographs, cephalometric images, Cone Beam Computed Tomography (CBCT), and intraoral cameras.

DENT 2.2. Complies with relevant DICOM classes, including DICOM DX, DICOM CT, and DICOM SR and supports storing standardized image formats such as DICOM and DICOM SR to ensure interoperability and consistent data exchange.

DENT 3. Reporting, Workflow, and Tools Requirements

DENT 3.1. Provides customizable structured reporting templates tailored for general dentistry, endodontics, orthodontics, and other dental specialties.

DENT 3.2. Offers tools for tagging and annotating clinical details such as tooth number, arch, and quadrant, with functionality for longitudinal image comparison to track changes over time.

DENT 3.3. Delivers customizable workflow management features, including study assignment, status tracking, and turnaround monitoring, to optimize clinical efficiency.

DENT 3.4. Provides advanced measurement tools for clinical analysis, including root canal length, bone density, and other quantitative assessments.

DENT 3.5. Integrates with voice recognition and natural language processing platforms to streamline reporting and documentation.

DENT 4. Image Display and Analysis Requirements

DENT 4.1. Supports intuitive navigation by quadrant and individual tooth for precise clinical review.

DENT 4.2. Provides advance CBCT analysis tools, including multiplanar reconstruction (MPR), 3D rendering, implant planning, and nerve canal tracing, to support comprehensive diagnostic evaluation and treatment planning.

DENT 4.3. Enables side-by-side comparison of serial imaging studies with synchronization and alignment features for longitudinal assessment.

DENT 4.4. Support dental hanging protocols such as FMX18, 4BWX, PX, DX, etc.

DENT 5. Security and Compliance Requirements

DENT 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

DENT 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

DENT 5.3 Encrypts all Protected Health Information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

DENT 5.4. Complies with all applicable privacy and security regulations, including HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools.

DENT 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

DENT 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

DENT 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

DENT 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

DENT 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

DENT 6. Interoperability Requirements

DENT 6.1. Supports Integrating the Healthcare Enterprise (IHE) profiles relevant to dental workflows, including Scheduled Workflow (SWF) and Evidence Documents (ED), to ensure standardized communication and documentation.

DENT 6.2. Enables secure image sharing and collaboration among multidisciplinary teams, including orthodontists, oral surgeons, prosthodontists, and general dentists, with access controls and encrypted transmission.

DENT 6.3. Provides remote access capabilities to support tele-dentistry consultations, enabling authorized users to view, annotate, and discuss imaging studies from distributed locations.

DENT 6.4. Supports DICOM Modality Worklist (MWL) and Modality Performed Procedure Step (MPPS) to ensure accurate patient/worklist synchronization and automated workflow integration across dental imaging devices.

DENT 6.5. Supports DICOM Structured Reporting (SR) for dental findings, measurements, and annotations to enable standardized documentation and downstream clinical data use.

DENT 6.6. Supports interoperability with Cone Beam Computed Tomography (CBCT) systems, including full DICOM 3D dataset ingestion, visualization, and export.

DENT 7. System Performance and Availability Requirements

DENT 7.1 Provides rapid acquisition, rendering, and playback of dental imaging modalities (including intraoral radiographs, panoramic studies, cephalometric images, and CBCT volumes) with low latency and smooth visualization to support timely clinical assessment and chairside treatment planning.

DENT 7.2 Supports scalable performance to accommodate increasing volumes of dental studies, concurrent users across operatories, and expanding imaging modalities without degradation in responsiveness or image quality.

DENT 7.3 Enables efficient access to archived studies (e.g., intraoral series, panoramic images, cephalometric studies, and CBCT datasets), to support diagnostic review, treatment planning, and multi-visit continuity of care.

DENT 7.4 Optimizes performance across dental-specific environments including operatory workstations, mobile consultation devices, tablets, and front-office review stations, ensuring consistent image clarity, rendering speed, and user responsiveness.

DENT 7.5 Includes performance monitoring dashboards and analytics tailored to dental imaging workflows, providing visibility into system health, rendering performance, CBCT reconstruction times, response times, and usage patterns across operatories and clinics.

DENT 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring continuity of imaging access during active patient encounters.

DENT 7.7 Implements a high-availability architecture and disaster recovery design that ensures uninterrupted dental clinical operations (including imaging acquisition, chairside review, and treatment planning) across single-site and multi-clinic environments, delivering a minimum of 99.9% system uptime.

DENT 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting dental image acquisition, rendering, or retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

DENT 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to dental imaging workflows, including intraoral acquisition, panoramic and cephalometric rendering, and CBCT dataset retrieval. All test results shall be logged and made available for audit and compliance review.

DENT 8. Online Availability, Portability, and Imaging Alignment

DENT 8.1. Provides secure, web-accessible functionality to enable authorized users to access dental imaging studies, reports, and workflows from any location, supporting remote clinical operations and tele-dentistry services.

DENT 8.2. Supports portability of dental treatment plans, including the ability to import, export, and share orthodontic treatment objects, implant planning files, and prosthodontic design data across institutions and platforms in compliance with DICOM standards.

DENT 8.3. Enables seamless consultation workflows by allowing multidisciplinary teams to access synchronized imaging data, treatment plans, and annotations during case reviews, peer consultations, and collaborative planning sessions.

DENT 8.4. Maintains alignment with the broader imaging ecosystem, including diagnostic radiology, oral pathology, and surgical planning systems, to ensure unified patient views and continuity of care across dental disciplines.

DENT 8.5. Provides mechanisms for real-time data synchronization and version control to prevent discrepancies between imaging studies and treatment planning data during collaborative review and decision-making.

DENT 9. Server-Side Rendering Requirements

DENT 9.1. Supports server-side rendering of dental images to enable efficient viewing and manipulation of large CBCT and panoramic datasets without requiring full client-side downloads.

DENT 9.2. Delivers rendered images to client devices via secure streaming protocols, ensuring responsive performance across varied network conditions and device types.

DENT 9.3. Provides advanced visualization features through server-side rendering, including multiplanar reconstruction (MPR), 3D rendering, implant simulation, cine loop playback, and quantitative overlays, with minimal latency.

DENT 9.4. Optimizes server resources to support concurrent users and high-throughput workflows typical of dental practices, including case reviews and remote consultations.

DENT 9.5. Includes failover and load-balancing mechanisms to maintain rendering performance and availability during peak usage or infrastructure disruptions.

DENT 10. Augmented Intelligence (AI) Requirements

DENT 10.1. Integrates AI tools capable of performing tooth detection, segmentation, and volumetric analysis to support diagnostic and treatment planning workflows.

DENT 10.2. Supports lesion and pathology tracking across serial imaging studies, enabling longitudinal assessment of caries progression, periodontal disease, and treatment response.

DENT 10.3. Automates dental-specific measurements, including root canal length, alveolar bone density, and orthodontic alignment metrics, in compliance with established clinical standards.

DENT 10.4. Provides AI-generated insights to assist in evaluating treatment response, disease progression, and differential diagnosis, with contextual relevance to dental specialties.

DENT 10.5. Delivers confidence scoring and explainable rationale for all AI-generated outputs, ensuring transparency and interpretability for clinical users.

DENT 10.6. Ensures mechanisms for human oversight and validation of AI-generated content, including the ability to review, edit, and approve findings prior to clinical use.

DENT 10.7. Supports customization of AI behavior and output based on institutional protocols, clinical workflows, and user-defined parameters.

DENT 10.8. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

DENT 10.9. Validation of AI algorithms against diverse datasets to ensure accuracy across patient demographics.

SOW - Dermatology

The vendor shall provide a comprehensive Dermatology Picture Archiving and Communication System (PACS) designed to support dermatologic imaging workflows across clinical, surgical, and research settings. The Dermatology PACS shall include all necessary components, software, licensing, and incidental support services, to deliver a fully integrated data and imaging management platform.

DERM 1. General System Requirements.

DERM 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

DERM 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

DERM 1.3. Utilizes vendor-neutral architecture and comply with interoperability standards including DICOM for imaging data, HL7 for clinical messaging, and FHIR for RESTful data exchange.

DERM 1.4. Provides scalable infrastructure to accommodate increasing imaging volumes and the evolving needs of Dermatology services, including advanced imaging modalities and data-intensive workflows.

DERM 1.5. Integrates with Dermatology-specific diagnostic tools to support tumor characterization, treatment planning, and longitudinal disease tracking.

DERM 1.6. Provides flexible and secure storage options, including support for lossless image compression and robust metadata indexing to enable efficient retrieval and analysis.

DERM 2. Imaging Modality Support Requirements.

DERM 2.1. Securely receives and archives high-resolution dermatologic images, including clinical photography, dermoscopy, confocal microscopy, Total Body Photograph (TBP) and multispectral imaging.

DERM 2.2. Compliance with DICOM Visible Light (VL) for dermatology imaging and DICOM Structured Reporting (SR) to support standardized documentation, lesion tracking, and interoperability across clinical systems.

DERM 2.3. Supports a wide range of standardized image formats including DICOM, JPEG, PNG, TIFF, and MP4 to accommodate dermoscopy, clinical photography, and video documentation.

DERM 2.4. Provides compatibility with DICOM web services (WADO-RS, QIDO-RS, STOW-RS) for seamless web-based access, query, and storage of dermatology images.

DERM 2.5. Enables ingestion and archiving of multimodal dermatology data, including dermoscopy, confocal microscopy, histopathology images, and clinical photographs.

DERM 2.6. Supports structured metadata capture (e.g., lesion location, body mapping, device ID, acquisition parameters) to enhance searchability and longitudinal tracking.

DERM 2.7. Provides lossless and lossy compression options optimized for dermatology imaging to balance storage efficiency with diagnostic quality.

DERM 3. Reporting, Workflow, and Tools Requirements

DERM 3.1. Provides standardized, structured reporting templates tailored to dermatology subspecialties (e.g., pigmented lesions, inflammatory conditions, wound care, cosmetic dermatology).

DERM 3.2. Offers advanced annotation, measurement, and markup tools (e.g., diameter, asymmetry, border irregularity, color analysis, vascular pattern mapping).

DERM 3.3. Enables side-by-side comparison of dermatologic images over time, supporting longitudinal assessment of lesion evolution and treatment response.

DERM 3.4. Includes quantitative metrics for lesion morphology, color distribution, vascular patterns, and texture analysis to support objective evaluation.

DERM 3.5. Provides customizable workflow management tools (e.g., study assignment, status tracking, turnaround monitoring, escalation alerts).

DERM 3.6. Supports longitudinal tracking of skin conditions with lesion mapping, body-surface diagrams, and integration with TBP.

DERM 3.7. Facilitates secure multidisciplinary collaboration, remote dermatology consultations, and seamless data exchange with referring providers and specialists.

DERM 3.8. Integrates with voice recognition and natural language processing Natural Language Processing (NLP) platforms to streamline reporting and reduce documentation burden.

DERM 3.9. Provides customizable dashboards and analytics tools for monitoring workflow performance, resource utilization, and quality metrics.

DERM 4. Image Display and Analysis Requirements

DERM 4.1. Supports advanced visualization including 3D skin surface rendering, multispectral imaging, and hyperspectral analysis for enhanced diagnostic accuracy.

DERM 4.2. Provides lesion tracking, zoom functionality, and side-by-side comparison of serial images, dermoscopic views, and multimodal datasets.

DERM 4.3. Ensures compatibility with TBP and mole-mapping systems for comprehensive skin surveillance.

DERM 4.4. Auto-populates measurements, annotations, and findings into structured reports to reduce manual entry and improve accuracy.

DERM 4.5. Offers advanced image analysis tools including automated lesion segmentation, border detection, and volumetric measurement.

DERM 4.6. Integrates AI-assisted diagnostic support for lesion classification (e.g., melanoma risk scoring, inflammatory condition detection).

DERM 4.7. Provides customizable display layouts and user preferences to adapt to dermatology subspecialty workflows.

DERM 4.8. Enables mobile access for bedside, clinic, and tele-dermatology environments.

DERM 4.9. Includes performance monitoring and image quality assurance tools (e.g., lighting correction, focus validation).

DERM 5. Security and Compliance Requirements

DERM 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

DERM 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

DERM 5.3 Encrypts all Protected Health Information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

DERM 5.4 Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools

DERM 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

DERM 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

DERM 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

DERM 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

DERM 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

DERM 6. Interoperability Requirements

DERM 6.1. Provides bi-directional data exchange, allowing dermatology images, structured reports, and metadata to flow into EHRs while retrieving patient demographics, orders, and prior imaging studies.

DERM 6.2. Allows customizable integration profiles to adapt to local workflows, including dermatology-specific reporting templates, lesion tracking protocols, and oncology pathways.

DERM 7. System Performance and Availability Requirements

DERM 7.1 Provides rapid acquisition, rendering, and display of dermatology imaging modalities (including dermatoscopic images, total-body photography, multispectral imaging, and high-resolution clinical photographs) with low latency to support timely assessment and lesion evaluation.

DERM 7.2 Supports scalable performance to accommodate increasing volumes of dermatologic images, high-resolution datasets, concurrent users across exam rooms, and expanding imaging applications without degradation in responsiveness or image quality.

DERM 7.3 Enables efficient access to archived studies (e.g., dermatoscopic images, total-body photography sessions, lesion-tracking series), to support longitudinal comparison and clinical decision-making.

DERM 7.4 Optimizes performance across dermatology-specific environments (including exam-room workstations, mobile consultation devices, tablets, and tele-dermatology platforms) ensuring consistent image clarity, zoom responsiveness, and high-resolution rendering.

DERM 7.5 Includes performance monitoring dashboards and analytics tailored to dermatology workflows, providing visibility into system health, rendering performance, response times, and usage patterns across clinics and tele-dermatology services.

DERM 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to dermatologic imaging during active patient encounters.

DERM 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous dermatology clinical operations (including image acquisition, lesion comparison, and tele-dermatology review) across single-site and multi-clinic environments, delivering a minimum of 99.9% system uptime.

DERM 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting dermatologic image acquisition, rendering, or retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

DERM 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to dermatology workflows, including dermatoscopic image retrieval, total-body photography access, and longitudinal comparison tools. All test results shall be logged and made available for audit and compliance review.

DERM 8. Augmented Intelligence (AI) Requirements

DERM 8.1. Provides AI-assisted image analysis to automatically detect, classify, and highlight dermatologic findings (e.g., pigmented lesions, rashes, ulcers, inflammatory conditions).

DERM 8.2. Supports automated lesion segmentation, measurement (size, area, volume), and change detection over time to enable longitudinal tracking.

DERM 8.3. Delivers risk stratification tools for skin cancer screening (e.g., melanoma probability scoring) and triage of urgent cases.

DERM 8.4. Integrates with structured reporting workflows, auto-populating findings, measurements, and annotations into standardized dermatology templates.

DERM 8.5. Provides real-time acquisition guidance with automated feedback on image quality, lighting, and focus to ensure diagnostically reliable images.

DERM 8.6. Enables multimodal analysis by combining dermoscopy, clinical photography, and histopathology images for comprehensive diagnostic support.

DERM 8.7. Ensures explainable AI outputs, including confidence scores, heatmaps, and rationale for automated findings to support clinician trust.

DERM 8.8. Provides customizable AI workflows tailored to subspecialties (e.g., pediatric dermatology, oncology, cosmetic dermatology).

DERM 8.9. Ensures compliance with regulatory frameworks (e.g., FDA, CE, HIPAA, GDPR) governing AI in medical imaging, including audit trails and validation processes.

DERM 8.10. Facilitates multidisciplinary collaboration by sharing AI-derived insights across PACS, EHRs, tele-dermatology platforms, and referring providers.

DERM 8.11. Provides analytics dashboards to monitor AI performance, accuracy, and usage patterns, supporting continuous improvement and quality assurance.

DERM 8.12 Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

SOW - Endoscopy

The vendor shall provide a comprehensive Endoscopic Picture Archiving and Communication System (PACS) designed to support real-time acquisition of endoscopic images and video, secure data archiving, and advanced analytics capabilities. The Endoscopy PACS shall include all required components, software, licensing, and associated support services, to deliver a fully integrated imaging and data management platform tailored to endoscopic workflows.

END 1. General System Requirements.

END 1.1 The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

END 1.2 The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

END 1.3 Utilizes vendor-neutral architecture and comply with interoperability standards including DICOM for imaging data, HL7 for clinical messaging, and FHIR for RESTful data exchange.

END 1.4 Scalable to support increasing imaging volumes, expanding endoscopy services, and multi-site deployments across networked facilities.

END 1.5 Incorporates a high-availability architecture with automated failover and comprehensive disaster recovery capabilities to ensure uninterrupted clinical operations and delivers 99.9% system uptime to support continuous access across outpatient clinics, hospitals, and tele health environments.

END 1.6 Supports advanced metadata-based search capabilities, allowing users to query studies using patient demographics, procedure type, date range, and other relevant attributes.

END 1.7 Offers tiered storage options with support for lossless compression and metadata indexing to optimize performance and retrieval efficiency.

END 2. Imaging Modality Support Requirements

END 2.1 Securely acquire and archive high-resolution images and videos from multiple endoscopic modalities, including gastroscopy, colonoscopy, bronchoscopy, and cystoscopy.

END 2.2 Fully compliant with DICOM SOP Classes, including support for Structured Reporting (DICOM SR), to ensure standardized documentation and interoperability and supports standardized image formats such as DICOM and DICOM SR for consistent data exchange and archival.

END 3. Reporting, Workflow, and Tools Requirements

END 3.1 Provide structured reporting templates tailored to endoscopic procedures, supporting standardized documentation and clinical interpretation.

END 3.2 Include tools for metadata tagging (e.g., patient ID, procedure type, anatomical region), image annotation, and longitudinal comparison of endoscopic studies.

END 3.3 Provide customizable workflow management tools, including study assignment, status tracking, and turnaround time monitoring, with support for role-based task allocation.

END 3.4 Support secure multidisciplinary collaboration, remote consultations, and encrypted data exchange with referring providers and specialists.

END 3.5 Integrate with voice recognition and/or natural language processing (NLP) platforms to streamline report generation and enhance documentation efficiency.

END 4. Image Display and Analysis Requirements

END 4.1 Support high-resolution image display with synchronized video playback, multi-frame navigation, and zoom/pan capabilities for detailed review.

END 4.2 Include trend analysis tools to evaluate procedural outcomes, anatomical changes, and disease progression over time.

END 4.3 Customizable display layouts, allowing users to configure image panels, annotation overlays, and metadata views based on clinical preferences.

END 5. Security and Compliance Requirements

END 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

END 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

END 5.3 Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

END 5.4 Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools

END 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

END 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

END 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

END 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

END 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

END 6. Interoperability Requirements

END 6.1 Supports standards-based interoperability required for exchanging orders, results, images, videos, procedure documentation, and clinical data with enterprise Electronic Health Record (EHR) systems.

END 6.2 Supports all relevant IHE Endoscopy and enterprise imaging integration profiles, including Scheduled Workflow (SWF), Evidence Documents (ED), and Cross-Enterprise Document Sharing (XDS/XDS-I) to ensure accurate, automated, and consistent workflow interoperability across endoscopy imaging, reporting, and documentation systems.

END 6.3 Provides DICOM Conformance Statements covering all DICOM functions of the proposed Endoscopy PACS solution, including support for DICOM Video, DICOM Encapsulated Documents (PDF), and DICOM Secondary Capture.

END 6.4 Supports HL7 v2.x messaging, including ORM, ORU, ADT, and SIU transactions, to enable standards-based order management, results reporting, and scheduling interoperability with enterprise EHR systems and procedure-room scheduling systems.

END 6.5 Supports DICOM Video Storage (MPEG-2, MPEG-4, H.264, or equivalent) and DICOM Image Storage for still captures, ensuring consistent, standards-based ingestion and retrieval of endoscopy video and image content from all major endoscopy systems.

END 6.6 Supports HL7 or FHIR-based exchange of structured procedure documentation, including findings, impressions, and coded terminology (e.g., SNOMED CT, LOINC), enabling seamless integration with the EHR and downstream analytics systems.

END 6.7 Supports interoperability with endoscopy reporting systems, procedure-room devices, and video capture systems through standards-based interfaces (DICOM, HL7, FHIR, or vendor-neutral APIs), ensuring consistent metadata, timestamps, and patient identifiers across all captured content.

END 7. System Performance and Availability

END 7.1 Provides rapid acquisition, rendering, and playback of endoscopic imaging modalities (including high-definition video, still-image captures, and intra-procedural annotations) with low latency and smooth, uninterrupted visualization to support real-time clinical assessment and procedural decision-making.

END 7.2 Supports scalable performance to accommodate increasing volumes of endoscopic procedures, high-resolution video datasets, concurrent users across procedure rooms, and expanding imaging applications without degradation in responsiveness or playback quality.

END 7.3 Enables efficient access to archived studies (e.g., GI, pulmonary, ENT, and surgical endoscopy videos and images), to support pre-procedure review, longitudinal comparison, and intra-procedural reference.

END 7.4 Optimizes performance across endoscopy-specific environments (including procedure-room workstations, mobile consultation devices, tablets, and remote review platforms) ensuring consistent video clarity, frame-rate stability, and responsive navigation through video timelines.

END 7.5 Includes performance monitoring dashboards and analytics tailored to endoscopy workflows, providing visibility into system health, video rendering performance, response times, storage throughput, and usage patterns across procedure rooms and clinical sites.

END 7.5 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to endoscopic imaging during active procedures and post-procedure documentation.

END 7.6 Implements a high-availability architecture and disaster recovery design that ensures continuous endoscopy clinical operations (including real-time video capture, image review, and reporting) across single-site and multi-clinic environments, delivering a minimum of 99.9% system uptime.

END 7.7 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting endoscopic video capture, rendering, or retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

END 7.8 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to endoscopy workflows, including high-definition video playback, still-image retrieval, and procedure documentation access. All test results shall be logged and made available for audit and compliance review.

END 8. Augmented Intelligence (AI) Requirements

END 8.1 Include integrated AI tools to assist with image and video analysis, including anatomical landmark detection, lesion identification, and classification of abnormalities (e.g., polyps, ulcers, strictures).

END 8.2 Support automated tagging and annotation of endoscopic findings, with contextual metadata such as anatomical region, lesion type, and severity indicators.

END 8.3 Provide AI-generated summaries and alerts for clinician review, including visual overlays, confidence scores, and traceable rationale to support diagnostic decision-making.

END 8.4 Provide explainable AI outputs, including transparent logic paths and reference frames, to ensure interpretability and clinical trust.

END 8.5 Mechanisms to ensure human oversight of AI-assisted interpretations, including manual validation, override capabilities, and audit logging of decisions.

END 8.6 Support customization based on institutional protocols, specialty-specific workflows, and user-defined parameters for adult and pediatric endoscopy.

END 8.7 Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

SOW - Nuclear Medicine

Vendor's products shall provide a comprehensive Nuclear Medicine Picture Archiving and Communication System (PACS) designed to support designed to support nuclear medicine imaging workflows across diagnostic, therapeutic, and research settings. The Nuclear Medicine PACS shall include all necessary components, software, licensing, and incidental support services, to deliver a fully integrated data and imaging management platform tailored to the unique needs of nuclear medicine.

NMED 1. General System Requirements.

NMED 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

NMED 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

NMED 1.3. Utilizes vendor-neutral architecture and comply with interoperability standards including DICOM for imaging data, HL7 for clinical messaging, and FHIR for RESTful data exchange.

NMED 1.4. Scalable to support increasing nuclear medicine imaging volumes, expanding molecular imaging services, and multi-site deployments across networked facilities.

NMED 1.5. Incorporates a high-availability architecture with automated failover and comprehensive disaster recovery capabilities to ensure uninterrupted clinical operations and delivers 99.9% system uptime to support continuous access across outpatient clinics, hospitals, and tele health environments.

NMED 1.6. Integrates diagnostic tools for quantification, segmentation, and treatment response assessment.

NMED 1.7. Offers tiered storage options with support for lossless compression and metadata indexing to optimize performance and retrieval efficiency.

NMED 2. Imaging Modality Support Requirements

NMED 2.1. Secures acquisition and archival of high-resolution nuclear medicine imaging modalities, including PET, SPECT, PET/CT, SPECT/CT, and gamma camera studies, with appropriate security and integrity controls.

NMED 2.2. Supports advanced nuclear imaging study types, including multi-frame, multi-phase, fusion, gated, and radiotracer-based functional imaging, ensuring compatibility with clinical and research workflows.

NMED 2.3. Fully compliant with DICOM SOP Classes, including support for Structured Reporting (DICOM SR) to ensure standardized documentation and interoperability, and supports standardized image formats such as DICOM and DICOM SR for consistent data exchange and archival.

NMED 3. Reporting, Workflow, and Tools Requirements.

NMED 3.1. Provides structured reporting templates for nuclear medicine protocols (e.g. PERCIST).

NMED 3.2. Provides tools for tagging and annotating with clinical details such as radiotracer type, dosage, and uptake values, and provides tools for comparing nuclear medicine images over time.

NMED 3.3. Supports IHE profiles such as Scheduled Workflow and Evidence Documents.

NMED 3.4. Provides customizable workflow management tools (e.g. study assignment, status tracking, turnaround monitoring).

NMED 3.5. Enables longitudinal tracking of radiotracer uptake and lesion mapping.

NMED 3.6. Supports secure multidisciplinary collaboration, tumor boards, remote nuclear medicine consultations, and data exchange with referring providers and specialists.

NMED 3.7. Integrates with voice recognition or natural language processing platforms.

NMED 4. Image Display and Analysis Requirements.

NMED 4.1. Supports multi-planar reconstruction (MPR).

NMED 4.2. Displays fusion images for PET/CT and SPECT/CT.

NMED 4.3. Includes tumor tracking tools with side-by-side image comparison.

NMED 4.4. Includes color mapping and radiotracer visualization.

NMED 4.5. Includes cine loop playback and gated image review.

NMED 4.6. Auto-populates radiotracer dosage, uptake values, and findings.

NMED 5. Security and Compliance Requirements.

NMED 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

NMED 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

NMED 5.3 Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

NMED 5.4 Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools

NMED 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

NMED 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

NMED 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

NMED 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

NMED 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

NMED 6. Interoperability Requirements.

NMED 6.1 Supports standards-based interoperability required for exchanging orders, results, images, quantitative data, with enterprise Electronic Health Record (EHR) systems.

NMED 6.2 Supports all relevant IHE Nuclear Medicine and enterprise imaging integration profiles, (e.g. Scheduled Workflow (SWF), NM Image Display (NM-ID), Evidence Documents (ED), and Cross-Enterprise Document Sharing for Imaging (XDS-I)), to ensure accurate, automated, and consistent workflow interoperability across nuclear medicine acquisition, processing, and reporting systems.

NMED 6.3 Provides DICOM Conformance Statements covering all DICOM functions of the proposed Nuclear Medicine PACS solution, including support for NM, PET, CT, MR, gated studies, dynamic acquisitions, and quantitative imaging objects.

NMED 6.4 Supports HL7 v2.x messaging, including ORM, ORU, ADT, and SIU transactions, to enable standards-based order management, results reporting, and scheduling interoperability with enterprise EHR systems.

NMED 6.5 Supports DICOM Nuclear Medicine Image Storage, PET Image Storage, and DICOM Enhanced NM/PET objects, including multi-frame datasets, gated series, dynamic acquisitions, and time-activity curves.

NMED 6.6 Supports DICOM Structured Reporting (SR) for nuclear medicine quantitative data, including SUV measurements, kinetic modeling outputs, and radiopharmaceutical administration details.

NMED 6.7 Supports interoperability with dose calibrators, and radiotracer administration systems through HL7, FHIR, or vendor-neutral APIs, ensuring accurate capture of administered dose, isotope, activity, and timing metadata.

NMED 6.8 Supports DICOM Modality Worklist (MWL), Modality Performed Procedure Step (MPPS), and Storage Commitment to ensure accurate, automated workflow interoperability across SPECT, PET, and hybrid imaging modalities.

NMED 6.9 Supports ingestion and retrieval of fused datasets (e.g., PET/CT, SPECT/CT, PET/MR) using standards-based DICOM multi-modality objects, ensuring consistent alignment, metadata integrity, and cross-system compatibility.

NMED 7. System Performance and Availability Requirements.

NMED 7.1 Provides rapid acquisition, rendering, and playback of nuclear medicine imaging modalities (including SPECT, PET, dynamic studies, gated acquisitions, and hybrid imaging datasets) with low latency and smooth visualization to support timely clinical interpretation and quantitative assessment.

NMED 7.2 Supports scalable performance to accommodate increasing volumes of nuclear medicine studies, large multi-series datasets, concurrent users across imaging suites, and expanding quantitative applications without degradation in responsiveness or reconstruction performance.

NMED 7.3 Enables efficient access to archived studies (e.g., SPECT, PET, gated cardiac studies, dynamic acquisitions, and hybrid imaging datasets), to support comparative review, longitudinal assessment, and protocol driven clinical decision making.

NMED 7.4 Optimizes performance across nuclear medicine–specific environments including reading room workstations, imaging suite consoles, mobile consultation devices, and multidisciplinary review platforms, ensuring consistent rendering quality, responsive navigation, and accurate display of quantitative data.

NMED 7.5 Includes performance monitoring dashboards and analytics tailored to nuclear medicine workflows, providing visibility into system health, reconstruction performance, response times, quantitative processing throughput, and usage patterns across imaging suites and clinical sites.

NMED 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to nuclear medicine imaging during active acquisition, processing, and interpretation.

NMED 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous nuclear medicine clinical operations (including image acquisition, reconstruction, quantitative analysis, and reporting) across single-site and multi-facility environments, delivering a minimum of 99.9% system uptime.

NMED 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting nuclear medicine image acquisition, reconstruction, rendering, or retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

NMED 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to nuclear medicine workflows, including SPECT and PET dataset retrieval, hybrid imaging access, and quantitative processing continuity. All test results shall be logged and made available for audit and compliance review.

NMED 8. Augmented Intelligence (AI) Requirements

NMED 8.1. Integrates AI algorithms for lesion detection, quantification, and classification across PET, SPECT, PET/CT, and SPECT/CT studies.

NMED 8.2. Supports automated segmentation of organs, tissues, and regions of interest, including gated and multi-phase acquisitions.

NMED 8.3. Provides AI-driven quantification tools for radiotracer uptake, standardized uptake values, kinetic modeling, and treatment response assessment.

NMED 8.4. Provides AI-assisted fusion and registration of nuclear medicine images with CT, MRI, or pathology datasets to enhance diagnostic accuracy.

NMED 8.5. Provides configurable confidence scoring and explainability features for all AI-generated findings.

NMED 8.6. Integrates AI outputs into structured reporting, annotations, and case review workflows.

NMED 8.7. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

NMED 8.8 Stores AI-generated artifacts (segmentations, overlays, derived images, structured findings) using open standards-based formats with full provenance tracking.

SOW - OB-GYN

The vendor shall provide a comprehensive Obstetrics & Gynecology (OB/GYN) Picture Archiving and Communication System (PACS) designed to support OB/GYN imaging workflows. The OB/GYN PACS shall include all necessary components, software, licensing, and incidental support services to deliver a fully integrated data and imaging management platform for prenatal screening, gynecologic diagnostics, and fertility care.

OBGYN 1. General System Requirements.

OBGYN 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

OBGYN 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

OBGYN 1.3. Utilizes vendor-neutral architecture and comply with interoperability standards including DICOM for imaging data, HL7 for clinical messaging, and FHIR for RESTful data exchange.

OBGYN 1.4. Provides scalable infrastructure to accommodate increasing imaging volumes and the evolving needs of POCUS services, including advanced imaging modalities and data-intensive workflows.

OBGYN 1.5. Integrates with diagnostic tools for quantification, segmentation, and treatment response assessment.

OBGYN 1.6. Provides flexible and secure storage options, including support for lossless image compression and robust metadata indexing to enable efficient retrieval and analysis.

OBGYN 2. Imaging Modality Support Requirements.

OBGYN 2.1. Securely receives and archives high-resolution images from multiple modalities, including 2D/D/4D ultrasound, MRI, CT hysteroscopy, and colposcopy.

OBGYN 2.2. Ingests real-time imaging data from fetal monitors and ultrasound machines.

OBGYN 2.3. Integrates with electronic feal monitoring systems and OB-specific devices such as Doppler and non-stress test (NST) equipment.

OBGYN 2.4. Compatible with prenatal screening protocols such as nuchal translucency (NT) scans, anomaly scans, and biophysical profiles

OBGYN 2.5. Complaint with DICOM standards for OB/GYN, including Structured Reporting (DICOM SR).

OBGYN 2.6. Provides metadata-based search and retrieval using patient ID, gestational age, imaging modality, or diagnosis.

OBGYN 2.7. Supports linking maternal and fetal records across multiple pregnancies.

OBGYN 3. Reporting, Workflow, and Tools Requirements.

OBGYN 3.1. Provides customizable structured reporting templates for prenatal scans, gynecologic exams, and fertility assessment.

OBGYN 3.2. Provides tools for tagging and annotating with clinical details.

OBGYN 3.3. Provides 3D/4D ultrasound visualization tools for assessing fetal anatomy and movement.

OBGYN 3.4. Provides customizable workflow management tools (e.g. study assignment, status tracking, turnaround monitoring) for sonographers, OB/GYNs, radiologists, and midwives.

OBGYN 3.5. Provides gynecologic imaging tools for evaluating the uterus, ovaries, and pelvic floor.

OBGYN 3.6. Supports secure multidisciplinary collaboration, remote consultations, and data exchange with referring providers and specialists.

OBGYN 4. Image Display and Analysis Requirements.

OBGYN 4.1. Provides OB-specific overlays, such as gestational age and biometric measurements (e.g., BPD, FL, HC, AC).

OBGYN 4.2. Supports side-by-side comparisons of serial scans to track fetal growth over time.

OBGYN 5. Compliance and Security Requirements.

OBGYN 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

OBGYN 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

OBGYN 5.3 Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

OBGYN 5.4. Complies with all applicable privacy and security regulations, including HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools.

OBGYN 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

OBGYN 5.6. Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

OBGYN 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

OBGYN 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

OBGYN 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

OBGYN 6. Interoperability Requirements

OBGYN 6.1 Enables bi-directional data exchange, allowing ultrasound findings, structured reports, and metadata to flow into EHRs while retrieving patient demographics, orders, and prior imaging studies.

OBGYN 6.2 Supports secure multidisciplinary collaboration through shared worklists, remote consultations, and interoperability with telemedicine platforms.

OBGYN 6.3 Provides customizable integration profiles to adapt to local workflows, including OB/GYN-specific reporting, prenatal protocols, and standardized templates.

OBGYN 6.4 Supports interoperability with mobile and tablet devices, enabling bedside access to prior studies, structured reports, and collaborative tools.

OBGYN 6.5 Facilitates future-proof extensibility, ensuring compatibility with emerging standards and evolving clinical interoperability requirements.

OBGYN 7. System Performance and Availability Requirements

OBGYN 7.1 Provides rapid acquisition, rendering, and playback of OBGYN imaging modalities (including obstetric ultrasound, fetal biometry, Doppler waveforms, gynecologic ultrasound, and 3D/4D fetal imaging) with low latency and smooth visualization to support timely clinical assessment and maternal-fetal decision-making.

OBGYN 7.2 Supports scalable performance to accommodate increasing volumes of obstetric and gynecologic studies, multi-series ultrasound datasets, concurrent users across exam rooms, and expanding imaging applications without degradation in responsiveness or rendering quality.

OBGYN 7.3 Enables efficient access to studies (e.g., prior obstetric ultrasounds, fetal growth assessments, Doppler studies, and gynecologic imaging), to support longitudinal pregnancy monitoring and comparative diagnostic evaluation.

OBGYN 7.4 Optimizes performance across OBGYN-specific environments (including ultrasound workstations, exam-room consoles, mobile consultation devices, tablets, and telehealth platforms) ensuring consistent image clarity, responsive navigation, and accurate display of fetal measurements and Doppler data.

OBGYN 7.5 Includes performance monitoring dashboards and analytics tailored to OBGYN imaging workflows, providing visibility into system health, rendering performance, response times, and usage patterns across clinics, maternal-fetal medicine units, and telehealth services.

OBGYN 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to OBGYN imaging during active examinations and maternal-fetal evaluations.

OBGYN 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous OBGYN clinical operations (including ultrasound acquisition, fetal growth assessment, Doppler analysis, and reporting) across single-site and multi-clinic environments, delivering a minimum of 99.9% system uptime.

OBGYN 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting OBGYN image acquisition, rendering, or retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

OBGYN 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to OBGYN workflows, including obstetric ultrasound retrieval, fetal growth comparison, Doppler waveform access, and 3D/4D rendering continuity. All test results shall be logged and made available for audit and compliance review.

OBGYN 8. Augmented Intelligence (AI) Requirements

OBGYN 8.1 Provides AI-assisted interpretation to automatically detect key OB/GYN findings (such as fetal anomalies, placental abnormalities, and uterine pathology).

OBGYN 8.2 Supports automated measurements including fetal biometry, amniotic fluid index, and cervical length, with clinician validation and override.

OBGYN 8.3 Provides real-time acquisition guidance including feedback on probe positioning, image quality, and completeness of exam protocols.

OBGYN 8.4 Integrates AI-generated findings, measurements, and annotations into structured reporting workflows and standardized templates.

OBGYN 8.5 Provides predictive analytics to support prenatal screening, treatment planning, and longitudinal maternal-fetal monitoring.

OBGYN 8.6 Supports natural language processing and voice interaction to streamline reporting and annotation.

OBGYN 8.7 Ensures explainable AI outputs, including confidence scores, visual overlays, and rationale for automated findings.

OBGYN 8.8 Ensures that deployed AI models operate as fixed, non learning systems in the clinical environment, while supporting structured user feedback capture for off site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

OBGYN 8.9 Stores AI generated artifacts (segmentations, overlays, derived images, structured findings) using open standards based formats with full provenance tracking.

SOW - Oncology

The vendor shall provide a comprehensive Radiation Oncology Picture Archiving and Communication System (PACS) that effectively supports imaging workflows across diagnostic, therapeutic, and research domains within Radiation Oncology. This system must encompass all essential elements, including software, licensing, and associated support services, to ensure a fully integrated platform for data and imaging management.

ONC 1. General System Requirements.

ONC 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

ONC 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

ONC 1.3. Provides scalable infrastructure to accommodate increasing imaging volumes and the evolving needs of Radiation Oncology services, including advanced imaging modalities and data-intensive workflows.

ONC 1.4. Integrates with oncology-specific diagnostic tools to support tumor characterization, treatment planning, and longitudinal disease tracking.

ONC 1.5. Provides flexible and secure storage options, including support for lossless image compression and robust metadata indexing to enable efficient retrieval and analysis.

ONC 2. Imaging Modality Support Requirements.

ONC 2.1. Supports a comprehensive range of imaging modalities used in Radiation Oncology, including but not limited to CT, MRI, PET/CT, SPECT/CT, Ultrasound, and digital Pathology.

ONC 2.2. Enables acquisition, storage, visualization, and analysis of images from these modalities in compliance with DICOM standards.

ONC 2.3. Supports advanced MRI techniques relevant to oncology, including diffusion-weighted imaging (DWI), perfusion imaging, and MR spectroscopy. These imaging types shall be viewable, quantifiable, and storable within the PACS environment.

ONC 2.4. Supports multi-frame, multi-phase, and gated imaging studies, including respiratory-gated and cardiac-gated acquisitions, with synchronized playback and analysis tools.

ONC 2.5. Complies with DICOM SOP Classes, including Structured Reporting (DICOM SR), Segmentation Objects, and Parametric Maps, to support quantitative imaging and AI-assisted workflows.

ONC 2.6. Enables integration with radiation treatment planning systems (TPS) and support import/export of RT-STRUCT, RT-PLAN, and RT-DOSE objects for seamless contouring and dose visualization.

ONC 3. Reporting, Workflow, and Tools Requirements.

ONC 3.1. Provides structured reporting templates tailored for Radiation Oncology, enabling standardized documentation of imaging findings, treatment response, and disease progression.

ONC 3.2. Includes tools for tagging, annotating, and comparing Oncologic images across serial studies to support longitudinal analysis and clinical decision-making.

ONC 3.3. Offers customizable workflow management tools, including study assignment, status tracking, and turnaround time monitoring, to optimize operational efficiency and reporting throughput.

ONC 3.4. Enables longitudinal tracking of tumors and lesion mapping across multiple timepoints, with visualization tools to assess treatment response and disease progression.

ONC 3.5. Supports secure collaboration among multidisciplinary teams, including tumor boards and remote oncology consultations, and facilitate data exchange with referring providers and specialists through encrypted channels.

ONC 4. Image Display and Analysis Requirements.

ONC 4.1. Supports multi-planar reconstruction (MPR) for cross-sectional imaging, enabling clinicians to visualize anatomical structures in axial, sagittal, and coronal planes.

ONC 4.2. Supports fusion image display for hybrid imaging studies, including PET/CT and SPECT/CT, with synchronized navigation and overlay capabilities.

ONC 4.3. The system shall support comprehensive tumor and lesion tracking across serial imaging studies, providing side-by-side comparison of images from multiple timepoints to enable longitudinal assessment of treatment response, disease progression, and tumor evolution.

ONC 4.4. Includes advanced visualization features such as customizable color mapping and radiotracer distribution overlays to enhance interpretation of functional imaging data.

ONC 4.5. Supports cine loop playback and gated image review for dynamic imaging studies, including respiratory and cardiac-gated acquisitions.

ONC 4.6. Quantitative analysis tools are available within the system, including region-of-interest (ROI) measurements, standardized uptake value (SUV) calculations, and functional volume estimation to support precision oncology workflows.

ONC 5. Security and Compliance Requirements.

ONC C 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

ONC 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

ONC 5.3 Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

ONC 5.4. Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools.

ONC 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

ONC 5.6. Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

ONC 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

ONC 5.8. Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

ONC 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

ONC 6. Interoperability Requirements

ONC 6.1. Support industry-standard interoperability protocols, including DICOM for imaging data exchange, HL7 for clinical messaging, and FHIR for RESTful integration with healthcare applications.

ONC 6.2. Support Integrating the Healthcare Enterprise (IHE) profiles relevant to oncology workflows, including Scheduled Workflow (SWF) and Evidence Documents (ED), to ensure standardized communication and documentation.

ONC 6.3. Enables secure image sharing and collaboration among multidisciplinary teams, including tumor boards and oncology specialists, with access controls and encrypted transmission.

ONC 6.4. Provides remote access capabilities to support tele-oncology consultations, enabling authorized users to view, annotate, and discuss imaging studies from distributed locations.

ONC 7. System Performance and Availability Requirements

ONC 7.1 Provides rapid acquisition, rendering, and playback of oncology imaging modalities (including CT, MR, PET/CT, SPECT/CT, ultrasound, and digital pathology images) with low latency and smooth visualization to support timely diagnostic interpretation, tumor assessment, and treatment planning.

ONC 7.2 Supports scalable performance to accommodate increasing volumes of oncology studies, large multimodality datasets, concurrent users across cancer centers, and expanding quantitative without degradation in responsiveness or rendering quality.

ONC 7.3 Enables efficient access to archived studies (e.g., prior CT, MR, PET, SPECT, ultrasound, and pathology images), to support longitudinal comparison, tumor response assessment, and multidisciplinary clinical decision-making.

ONC 7.4 Optimizes performance across oncology-specific environments (including radiology reading rooms, infusion centers, tumor board conference rooms, mobile consultation devices, and tele-oncology platforms) ensuring consistent image clarity, responsive navigation, and accurate display of tumor measurements and annotations.

ONC 7.5 Includes performance monitoring dashboards and analytics tailored to oncology workflows, providing visibility into system health, rendering performance, response times, dataset throughput, and usage patterns across cancer centers, imaging departments, and multidisciplinary teams.

ONC 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to oncology imaging during active interpretation, treatment planning, and multidisciplinary review.

ONC 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous oncology clinical operations (including multimodality image review, tumor response assessment, radiotherapy planning integration, and reporting) across single-site and multi-facility cancer care networks, delivering a minimum of 99.9% system uptime.

ONC 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting oncology image acquisition, rendering, retrieval, or quantitative analysis. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

ONC 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to oncology workflows, including multimodality dataset retrieval, longitudinal comparison tools, tumor measurement continuity, and radiotherapy planning data access. All test results shall be logged and made available for audit and compliance review.

ONC 8. Online Availability, Portability, and Imaging Alignment

ONC 8.1. Provide secure, web-accessible functionality to enable authorized users to access imaging studies, reports, and oncology workflows from any location, supporting remote clinical operations and tele-oncology services.

ONC 8.2. Support the portability of radiation treatment plans, including the ability to import, export, and share RT-STRUCT, RT-PLAN, and RT-DOSE objects across institutions and platforms in compliance with DICOM RT standards.

ONC 8.3. Enable seamless consultation workflows by allowing multidisciplinary teams to access synchronized imaging data, treatment plans, and annotations during tumor boards, peer reviews, and collaborative planning sessions.

ONC 8.4. Maintain alignment with the broader imaging ecosystem, including diagnostic radiology, nuclear medicine, and pathology systems, to ensure unified patient views and continuity of care across oncology disciplines.

ONC 8.5. Include mechanisms for real-time data synchronization and version control to prevent discrepancies between imaging studies and treatment planning data during collaborative review and decision-making.

ONC 9. Server-Side Rendering Requirements

ONC 9.1. Supports server-side rendering of medical images to enable efficient viewing and manipulation of large oncology datasets without requiring full client-side downloads.

ONC 9.2. Delivers rendered images to client devices via secure streaming protocols, ensuring responsive performance across varied network conditions and device types.

ONC 9.3. Supports server-side rendering, advanced visualization features including multi-planar reconstruction (MPR), fusion imaging, cine loop playback, and quantitative overlays, with minimal latency.

ONC 9.4. Optimizes server resources to support concurrent users and high-throughput workflows typical of radiation oncology environments, including tumor boards and remote consultations.

ONC 9.5. Includes failover and load-balancing mechanisms to maintain rendering performance and availability during peak usage or infrastructure disruptions.

ONC 10. Augmented Intelligence (AI) Requirements

ONC 10.1. Provides AI-assisted tumor detection, segmentation, and volumetric analysis to support diagnostic and treatment planning workflows.

ONC 10.2. Automate oncology-specific measurements, including RECIST (Response Evaluation Criteria in Solid Tumors) and PERCIST (PET Response Criteria in Solid Tumors), in accordance with established clinical standards.

ONC 10.3. Provides AI-generated insights to assist in evaluating treatment response, disease progression, and differential diagnosis, with relevance to radiation oncology.

ONC 10.4. Provides confidence scoring and explainable rationale for all AI outputs to ensure transparency and interpretability.

ONC 10.5. Supports customization of behavior and output based on institutional protocols, clinical workflows, and user-defined parameters.

ONC 10.6. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

ONC 10.7. Stores AI-generated artifacts (segmentations, overlays, derived images, structured findings) using open standards-based formats with full provenance tracking.

SOW - Ophthalmology

The vendor shall provide a comprehensive Ophthalmology Picture Archiving and Communication System (PACS) tailored for Ophthalmology imaging workflows. The Ophthalmology PACS shall include all necessary components, software, licensing, and incidental support services, to deliver a fully integrated data and imaging management platform tailored to the unique needs of ophthalmology.

OPH 1. General System Requirements

OPH 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

OPH 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

OPH 1.3. Utilizes a vendor-neutral architecture and complies with interoperability standards—including DICOM (for ophthalmic images, waveforms, and video), HL7 (for clinical messaging), and FHIR (for RESTful data exchange) —to ensure seamless integration with ophthalmic imaging devices, diagnostic instruments, EHR platforms, and enterprise imaging archives.

OPH 1.4. Provides scalable infrastructure to accommodate increasing volumes of studies, expanded service offerings, and multi-site deployments across networked facilities.

OPH 1.5. Incorporates a high availability architecture with automated failover and comprehensive disaster recovery capabilities to ensure uninterrupted clinical operations and delivers 99.9% system uptime to support continuous access across outpatient clinics, hospitals, and tele- health environments.

OPH 1.6. Supports integration with diagnostic tools supporting quantification, segmentation, and treatment response assessment.

OPH 1.7. Offers tiered storage options, including support for lossless compression and metadata indexing (e.g., eye laterality, modality, acquisition parameters).

OPH 2. Imaging Modality Support Requirements.

OPH 2.1. Receives and archives high-resolution images from Optical Coherence Tomography (OCT), fundus photography, fluorescein and indocyanine green angiography, corneal topography, Ultrasound Bio-Microscopy (UBM), and visual field testing.

OPH 2.2. Supports subspecialties such as retina, glaucoma, cornea, and anterior segment.

OPH 2.3. Complies with DICOM ophthalmic SOP classes, such as DICOM OCT and DICOM Structured Content.

OPH 2.4. Supports standardized image formats such as DICOM and DICOM SR.

OPH 3. Reporting, Workflow, and Tools Requirements.

OPH 3.1. Provides structured reporting templates for ophthalmologic subspecialities.

OPH 3.2. Offers tools for tagging and annotating with clinical details such as cup-to-disc ratio calculation and lesion size measurements, and provide tools for comparing images over time.

OPH 3.3. Supports IHE profiles such as Scheduled Workflow and Evidence Documents.

OPH 3.4. Provides customizable workflow management tools (e.g. study assignment, status tracking, turnaround monitoring).

OPH 3.5. Supports secure multidisciplinary collaboration and data exchange with referring providers and specialists.

OPH 3.6. Integrates with voice recognition or natural language processing platforms.

OPH 4. Image Display and Analysis Requirements.

OPH 4.1. Supports multi-planar reconstruction (MPR).

OPH 4.2. Provides side-by-side image comparison, multi-modal image comparison, and overlay views.

OPH 4.3. Supports cine loop playback and gated image review.

OPH 4.4. Supports 3D rendering for volumetric OCT and corneal maps.

OPH 5. Security and Compliance Requirements.

OPH 5.1. Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

OPH 5.2. Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

OPH 5.3. Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

OPH 5.4. Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools.

OPH 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

OPH 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

OPH 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

OPH 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

OPH 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

OPH 6. Interoperability Requirements

OPH 6.1 Supports standards-based interoperability required for exchanging orders, results, images, waveforms, and ophthalmic measurements with enterprise Electronic Health Record (EHR) systems.

OPH 6.2 Supports all relevant IHE Eye Care integration profiles, including Eye Care Workflow (EYECARE-WF), Evidence Documents (ED), and Scheduled Workflow (SWF), to ensure accurate, automated, and consistent workflow interoperability across ophthalmic imaging, diagnostics, and reporting systems.

OPH 6.3 Provides DICOM Conformance Statements covering all DICOM functions including support for Ophthalmic Photography, OCT, OCT-A, Visual Field, Corneal Topography, and Encapsulated PDF objects.

OPH 6.4 Supports HL7 v2.x messaging, including ORM, ORU, ADT, and SIU transactions, to enable standards-based order management, results reporting, and scheduling interoperability with enterprise EHR systems and ophthalmology clinic management systems.

OPH 6.5 Supports DICOM Ophthalmic Image Storage SOP Classes, including: Ophthalmic Photography (color, red-free, autofluorescence); Ophthalmic Tomography (OCT, OCT-A); Ophthalmic Thickness Maps; Visual Field Test Results; Corneal Topography Maps; and Stereoscopic and multi-frame imaging

OPH 6.6 Supports DICOM Structured Reporting (SR) for ophthalmic measurements and findings, including retinal thickness maps, RNFL analysis, optic nerve parameters, and visual field indices.

OPH 6.7 Supports interoperability with ophthalmic diagnostic devices, including OCT, fundus cameras, visual field analyzers, topographers, and biometers, using standards-based interfaces (DICOM, HL7, FHIR, or vendor-neutral APIs) to ensure consistent metadata, patient identifiers, and measurement integrity.

OPH 6.8 Supports ingestion and retrieval of multi-modality ophthalmic datasets (e.g., OCT + fundus photo alignment, angiography sequences, stereo images) using standards-based DICOM objects to ensure cross-system compatibility and accurate longitudinal comparison

OPH 7. System Performance and Availability Requirements

OPH 7.1 Provides rapid acquisition, rendering, and display of ophthalmic imaging modalities (including OCT, OCT-A, fundus photography, fluorescein and ICG angiography, corneal topography, and visual field studies) with low latency and smooth visualization to support timely diagnostic interpretation and disease management.

OPH 7.2 Supports scalable performance to accommodate increasing volumes of ophthalmic studies, high-resolution multi-series datasets, concurrent users across exam rooms, and expanding imaging applications without degradation in responsiveness or rendering quality.

OPH 7.3 Enables efficient access to archived studies (e.g., OCT series, fundus images, angiography sequences, topography maps, and visual field results), to support longitudinal comparison, progression analysis, and clinical decision-making.

OPH 7.4 Optimizes performance across ophthalmology-specific environments (including diagnostic imaging workstations, exam-room consoles, mobile consultation devices, tablets, and tele-ophthalmology platforms) ensuring consistent image clarity, responsive navigation, and accurate display of quantitative measurements.

OPH 7.5 Includes performance monitoring dashboards and analytics tailored to ophthalmology workflows, providing visibility into system health, rendering performance, response times, dataset throughput, and usage patterns across clinics and imaging suites.

OPH 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to ophthalmic imaging during active examinations and diagnostic review.

OPH 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous ophthalmology clinical operations (including OCT review, fundus image comparison, angiography interpretation, and visual field analysis) across single-site and multi-clinic environments, delivering a minimum of 99.9% system uptime.

OPH 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting ophthalmic image acquisition, rendering, or retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

OPH 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to ophthalmology workflows, including OCT dataset retrieval, fundus image access, angiography sequence playback, and visual field data continuity. All test results shall be logged and made available for audit and compliance review.

OPH 8. Augmented Intelligence (AI) Requirements

OPH 8.1. Provides AI-assisted ophthalmic image analysis, including retinal layer segmentation, optic nerve head evaluation, vascular mapping, and lesion detection in accordance with established imaging guidelines.

OPH 8.2. Supports automated detection and classification of ophthalmic disorders such as diabetic retinopathy, glaucoma, age-related macular degeneration, retinal detachment, and keratoconus, with configurable diagnostic thresholds.

OPH 8.3. Provides AI-generated summaries, alerts, annotations and visual indicators with contextual explanations for clinician and technician reviews.

OPH 8.4. Provides confidence scoring and explainable rationale for all AI outputs, including traceable logic and reference to OCT or fundus image evidence.

OPH 8.5. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

OPH 8.6. Stores AI-generated artifacts (segmentations, overlays, derived images, structured findings) using open standards-based formats with full provenance tracking.

SOW - Pathology

The vendor shall offer a comprehensive Pathology Picture Archiving and Communication System (PACS) designed to support designed to support advanced digital pathology workflows. The Pathology PACS shall include all necessary components, software, licensing, and incidental support services—to deliver a fully integrated data and imaging management platform.

PATH 1. General System Requirements.

PATH 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

PATH 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

PATH 1.3. Utilizes vendor-neutral architecture and comply with interoperability standards including DICOM for imaging data, HL7 for clinical messaging, and FHIR for RESTful data exchange.

PATH 1.4. Scalable to support increasing digital pathology imaging volumes, expanding pathology services such as whole-slide imaging and computational pathology workflows, and multi-site deployments across networked laboratory and clinical facilities.

PATH 1.5. Incorporates a high-availability architecture with automated failover and comprehensive disaster recovery capabilities to ensure uninterrupted clinical operations and delivers 99.9% system uptime to support continuous access across outpatient clinics, hospitals, and tele health environments.

PATH 1.6. Integrates with diagnostic tools for quantification, segmentation, and treatment response assessment.

PATH 1.7. Offers tiered storage options with support for lossless compression and metadata indexing to optimize performance and retrieval efficiency.

PATH 1.8. Offers search and retrieval functions that deliver access by patient ID, specimen type, diagnosis, and/or date, supporting efficient case review.

PATH 1.9. Supports DICOM Supplement 145 for Whole Slide Imaging (WSI) and complies with ISO 15189, ensuring adherence to international pathology imaging standards.

PATH 2. Imaging Modality Support Requirements.

PATH 2.1. Secure acquisition and archival of imaging data from whole slide imaging (WSI), gross imaging cameras, and digital microscopes, with appropriate security controls to protect patient and specimen information.

PATH 2.2. Provides support for multiple pathology imaging domains, including WSI, histopathology, cytology, and molecular diagnostics, ensuring compatibility with diverse clinical workflows.

PATH 2.3. Compliant with DICOM SOP Classes, including Structured Reporting (DICOM SR), to enable standardized documentation, interoperability, and integration with enterprise imaging systems.

PATH 2.4. Supports non-DICOM acquisition including TIFF, SVS, NDPI , enabling ingestion and management of images from diverse pathology imaging devices.

PATH 3. Reporting, Workflow, and Tools Requirements.

PATH 3.1. Provides customizable structured reporting templates for histopathology, cytology, and molecular pathology.

PATH 3.2. Provides tools for tagging and annotating for marking regions of interest, performing measurements, and grading.

PATH 3.3. Provides customizable workflow management tools (e.g. study assignment, status tracking, turnaround monitoring).

PATH 3.4. Supports barcode scanning for specimen tracking and slide identification.

PATH 3.5. Supports secure multidisciplinary collaboration, remote consultations, and data exchange with referring providers and specialists.

PATH 3.6. Integrates with voice recognition or natural language processing platforms.

PATH 4. Image Display and Analysis Requirements.

PATH 4.1. Capable of high-speed zoom and pan functionality when handling gigapixel pathology images.

PATH 4.2. Supports multi-layered image visualization, such as immunohistochemistry overlays.

PATH 4.3. Supports comparison of serial sections or historical cases side-by-side.

PATH 5. Security and Compliance Requirements.

PATH 5.1. Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

PATH 5.2. Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

PATH 5.3. Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

PATH 5.4. Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools.
PATH 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

PATH 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

PATH 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

PATH 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

PATH 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

PATH 6. Interoperability Requirements

PATH 6.1 Supports standards-based interoperability required for exchanging orders, results, whole-slide images, annotations, and pathology reports with enterprise Electronic Health Record (EHR) systems and Laboratory Information Systems (LIS).

PATH 6.2 Supports all relevant IHE Pathology and enterprise imaging integration profiles, including Anatomic Pathology Workflow (APW), Evidence Documents (ED), and Cross-Enterprise Document Sharing (XDS/XDS-I), to ensure accurate, automated, and consistent workflow interoperability across pathology imaging, LIS systems, and reporting platforms.

PATH 6.3 Provides DICOM Conformance Statements covering all DICOM functions, including support for Whole Slide Imaging (WSI), multi-frame images, z-stacked images, fluorescence microscopy, and DICOM Encapsulated PDF.

PATH 6.4 Supports HL7 v2.x messaging, including ORM, ORU, ADT, and specimen-related segments (SPM, OBX), to enable standards-based order management, results reporting, specimen tracking, and demographic interoperability with LIS and enterprise EHR systems.

PATH 6.5 Supports DICOM Whole Slide Image (WSI) Storage SOP Classes, including tiled, multi-resolution, and multi-frame images, ensuring consistent, standards-based ingestion and retrieval of digital slides from all major pathology scanners.

PATH 6.6 Supports DICOM Structured Reporting (SR) for pathology annotations, measurements, Region-of-Interest (ROI) metadata, and quantitative image analysis outputs, enabling consistent exchange of structured diagnostic information.

PATH 6.7 Supports interoperability with pathology scanners, image analysis systems, and LIS platforms through standards-based interfaces (DICOM, HL7, FHIR, or vendor-neutral APIs), ensuring consistent metadata, specimen identifiers, staining information, and slide-level attributes.

PATH 6.8 Supports ingestion and retrieval of multi-modal pathology datasets, including brightfield, fluorescence, z-stacked, and multi-channel images, using standards-based DICOM objects to ensure cross-system compatibility and accurate longitudinal comparison.

PATH 7. System Performance and Availability Requirements

PATH 7.1 Provides rapid acquisition, rendering, and display of pathology imaging modalities (including Whole-Slide Images (WSI), z-stacked images, fluorescence microscopy, and high-resolution digital slides) with low latency and smooth navigation to support timely diagnostic interpretation and case review.

PATH 7.2 Supports scalable performance to accommodate increasing volumes of digital pathology studies, extremely large multi-gigapixel datasets, concurrent users across pathology labs, and expanding quantitative applications without degradation in responsiveness or rendering quality.

PATH 7.3 Enables efficient access to archived studies (e.g., whole-slide images, immunohistochemistry series, fluorescence images, and historical case materials), to support comparative review, longitudinal assessment, and multidisciplinary clinical decision-making.

PATH 7.4 Optimizes performance across pathology-specific environments (e.g. high-resolution diagnostic workstations, laboratory review stations, mobile consultation devices, tumor board conference rooms, and telepathology platforms), ensuring consistent image clarity, responsive zooming and panning, and accurate display of annotations and measurements.

PATH 7.5 Includes performance monitoring dashboards and analytics tailored to pathology workflows, providing visibility into system health, rendering performance, response times, dataset throughput, and usage patterns across pathology labs and multidisciplinary teams.

PATH 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to pathology imaging during active diagnostic review and multidisciplinary case preparation.

PATH 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous pathology clinical operations (including whole-slide image review, quantitative analysis, and reporting) across single-site and multi-facility laboratory networks, delivering a minimum of 99.9% system uptime.

PATH 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting pathology image acquisition, rendering, retrieval, or quantitative processing. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

PATH 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to pathology workflows, including whole-slide image retrieval, z-stack access, fluorescence image continuity, and quantitative analysis availability. All test results shall be logged and made available for audit and compliance review.

PATH 8. Augmented Intelligence (AI) Requirements

PATH 8.1. Integrates AI algorithms for detection, classification, and quantification of histopathologic features.

PATH 8.2. Supports automated segmentation of tissue regions, cellular structures, and biomarkers to enhance diagnostic accuracy and reproducibility.

PATH 8.3. Provides AI-driven tools for treatment response assessment, prognostic scoring, and predictive modeling.

PATH 8.4. Stores AI-generated artifacts (segmentations, overlays, derived images, structured findings) using open standards-based formats with full provenance tracking.

PATH 8.5. Integrates AI outputs into structured reporting, annotations, and case review workflows.

PATH 8.6. Provides performance monitoring and audit capabilities for AI models, including accuracy tracking, drift detection, and usage reporting.

PATH 8.7. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

SOW - POCUS

The vendor shall provide a comprehensive Point-of-Care Ultrasound (POCUS) Picture Archiving and Communication System (PACS) designed to support ultrasound imaging workflows across diagnostic, procedural, and bedside care settings. The POCUS PACS shall include all necessary components, software, licensing, and incidental support services, to deliver a fully integrated imaging management platform tailored to the unique demands of POCUS in emergency medicine, critical care, internal medicine, and other clinical environments.

POCUS 1. General System Requirements.

POCUS 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

POCUS 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

POCUS 1.3. Utilizes vendor-neutral architecture and comply with interoperability standards including DICOM for imaging data, HL7 for clinical messaging, and FHIR for RESTful data exchange.

POCUS 1.4. Provides scalable infrastructure to accommodate increasing imaging volumes and the evolving needs of POCUS services, including advanced imaging modalities and data-intensive workflows.

POCUS 1.5. Integrates with diagnostic tools for quantification, segmentation, and treatment response assessment.

POCUS 1.6. Provides flexible and secure storage options, including support for lossless image compression and robust metadata indexing to enable efficient retrieval and analysis.

POCUS 2. Imaging Modality Support Requirements.

POCUS 2.1. Securely receives and archives high-resolution ultrasound images and video clips acquired at the point of care, including cardiac, abdominal, musculoskeletal, vascular, pulmonary, and obstetric/gynecologic applications.

POCUS 2.2. Accommodates both cart-based and handheld ultrasound devices, enabling seamless data capture and transfer from a variety of hardware sources

POCUS 2.3. Enables real-time image acquisition with secure archiving and rapid retrieval for efficient clinical workflows.

POCUS 2.4. Complies with DICOM SOP Classes, including Structured Reporting (DICOM SR), Segmentation Objects, and Parametric Maps, to support quantitative imaging and AI-assisted workflows.

POCUS 2.5. Supports standardized image formats such as DICOM, JPEG, and MP4.

POCUS 2.6. Ingests and archives still images, cine loops, and audio annotations from POCUS exams.

POCUS 3. Reporting, Workflow, and Tools Requirements.

POCUS 3.1. Provides standardized, structured reporting templates (e.g., FAST exam, cardiac, lung, vascular) to ensure consistency, accuracy, and interoperability across clinical settings.

POCUS 3.2. Offers advanced tools for tagging, annotating (e.g., length, area, volume), labeling, and temporal comparison to support quantitative analysis and longitudinal assessment.

POCUS 3.3. Enables automatic routing, indexing, and categorization of images and reports based on device ID, user credentials, patient demographics, or predefined clinical workflows.

POCUS 3.4. Delivers customizable workflow management capabilities, including study assignment, status tracking, turnaround monitoring, and escalation alerts to optimize efficiency.

POCUS 3.5. Supports longitudinal tracking of findings, enabling clinicians to monitor disease progression, treatment response, and patient outcomes over time.

POCUS 3.6. Facilitates secure, multidisciplinary collaboration through remote consultations, shared worklists, and seamless data exchange with referring providers and specialists.

POCUS 3.7. Integrates with voice recognition and natural language processing (NLP) platforms to streamline reporting, reduce documentation burden, and enhance clinical productivity.

POCUS 3.8. Provides customizable dashboards and analytics tools for monitoring workflow performance, resource utilization, and quality metrics.

POCUS 3.9. Ensures audit trails, role-based access controls, and compliance with regulatory standards (e.g., HIPAA, GDPR) to safeguard patient data and maintain accountability.

POCUS 3.10. Supports interoperability with electronic health records (EHRs), POCUS information systems, and other clinical platforms via HL7, FHIR, and DICOM standards.

POCUS 4. Image Display and Analysis Requirements.

POCUS 4.1. Provides real-time image display with smooth playback of cine loops, ensuring immediate visualization at the point of care.

POCUS 4.2. Supports side-by-side and multi-panel longitudinal assessments, enabling comparison of current and prior studies for disease progression or treatment response.

POCUS 4.3. Includes advanced cine loop playback options, gated image review (e.g., ECG-synchronized), and frame-by-frame navigation for precise analysis.

POCUS 4.4. Auto-populates findings, measurements, and annotations directly into structured reports, reducing documentation burden and improving accuracy.

POCUS 4.5. Optimizes user interface for mobile and tablet devices, ensuring intuitive bedside use in diverse clinical environments.

POCUS 4.6. Provides advanced visualization tools such as zoom, pan, dynamic contrast adjustment, and color Doppler overlays.

POCUS 4.7. Enables quantitative analysis features including strain imaging, volumetric measurements, and automated border detection.

POCUS 4.8. Supports customizable display layouts, dashboards, and user preferences to adapt to specialty-specific workflows.

POCUS 5. Security and Compliance Requirements.

POCUS 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

POCUS 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

POCUS 5.3 Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

POCUS 5.4. Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools.

POCUS 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

POCUS 5.6. Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

POCUS 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

POCUS 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

POCUS 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

POCUS 6. Interoperability Requirements.

POCUS 6.1. Provides bi-directional data exchange, allowing ultrasound findings, structured reports, and metadata to flow into EHRs while retrieving patient demographics, orders, and prior imaging studies.

POCUS 6.2. Supports secure multidisciplinary collaboration through shared worklists, remote consultations, and interoperability with telemedicine platforms.

POCUS 6.3. Allows customizable integration profiles to adapt to local workflows, including POCUS-specific reporting, trauma protocols, and templates.

POCUS 6.4. Supports interoperability with mobile and tablet devices, enabling bedside access to prior studies, structured reports, and collaborative tools.

POCUS 6.5. Facilitate future-proof extensibility, ensuring compatibility with emerging standards and evolving clinical interoperability requirements.

POCUS 7. Performance and Availability Requirements

POCUS 7.1. Provides rapid acquisition, rendering, and playback of point-of-care ultrasound imaging (including cardiac, abdominal, pulmonary, vascular, obstetric, and musculoskeletal studies), with low latency and smooth visualization to support immediate bedside clinical decision-making.

POCUS 7.2. Supports scalable performance to accommodate increasing volumes of POCUS studies, multi-site deployments, concurrent mobile users, and expanding clinical applications without degradation in responsiveness or image quality.

POCUS 7.3. Enables efficient access to archived studies (e.g., cardiac assessments, FAST exams, lung ultrasound, vascular access guidance, and procedural documentation), to support serial assessment, follow-up evaluation, and time-critical clinical workflows.

POCUS 7.4. Optimizes performance across POCUS-specific environments including handheld ultrasound devices, mobile phones, tablets, bedside workstations, emergency department consoles, and telehealth platforms, ensuring consistent image clarity, responsive navigation, and reliable playback in variable network conditions.

POCUS 7.5. Includes performance monitoring dashboards and analytics tailored to POCUS workflows, providing visibility into system health, response times, mobile device performance, network behavior, and usage patterns across emergency, inpatient, outpatient, and remote care settings.

POCUS 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to POCUS imaging during active bedside examinations and critical-care evaluations.

POCUS 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous POCUS clinical operations(including image acquisition, bedside review, procedural guidance documentation, and reporting) across single-site and multi-facility care networks, delivering a minimum of 99.9% system uptime.

POCUS 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting POCUS image acquisition, rendering, or retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

POCUS 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to POCUS workflows, including mobile device synchronization, bedside image retrieval, and procedural documentation continuity. All test results shall be logged and made available for audit and compliance review.

POCUS 8. Augmented Intelligence (AI) Requirements

POCUS 8.1. Provides AI-assisted image interpretation to automatically detect key findings such as effusion, pneumothorax, deep vein thrombosis, and cardiac function abnormalities.

POCUS 8.2. Supports automated quantitative measurements, including chamber dimensions, vessel diameter, volume, and strain analysis, with clinician validation and override.

POCUS 8.3. Provides real-time acquisition guidance, including feedback on probe positioning, image quality, and completeness of exam protocols.

POCUS 8.4. Integrates AI-generated findings, measurements, and annotations into structured reporting workflows and standardized templates.

POCUS 8.5. Provides predictive analytics to support triage, treatment planning, and longitudinal patient monitoring.

POCUS 8.6. Ensures explainable AI outputs, including confidence scores, visual overlays, and rationale for automated findings.

POCUS 8.7. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

POCUS 8.8 Stores AI-generated artifacts (segmentations, overlays, derived images, structured findings) using open standards-based formats with full provenance tracking.

SOW - Radiology

The vendor shall provide a comprehensive Radiology Picture Archiving and Communication System (DIN-PACS) designed to support real-time acquisition of radiologic images and studies, secure long-term data archiving, and advanced analytics capabilities. The Radiology DIN-PACS shall include all required hardware components, software applications, licensing, workstations and viewers (i.e. diagnostic and clinical) and associated support services necessary to deliver a fully integrated imaging and data management platform optimized for radiology workflows.

RAD 1. General System and Functionality Requirements

RAD 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

RAD 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

RAD 1.3. Provides a secure, scalable, and flexible infrastructure capable of supporting large imaging volumes across all radiology modalities while ensuring reliable preservation, rapid retrieval, and efficient management of all imaging data.

RAD 1.4. The system shall fully comply with all applicable DICOM standards across every implemented SOP Class and IOD, including complete preservation and transmission of all mandatory (Type 1 and Type 2) DICOM attributes. The vendor shall provide a comprehensive DICOM Conformance Statement covering all supported services, modalities, and objects, and shall validate all DICOM functions to ensure interoperability, accuracy, and suitability for use in regulated healthcare environments.

RAD 2. Imaging Modality Support

RAD 2.1. Supports multi-modality imaging and archiving across all standard radiology modalities, including advanced modalities such as digital breast tomosynthesis, dual-energy CT, functional MRI, PET/CT and PET/MR.

RAD 2.2. Delivers standards-based DICOM reception of real-time imaging data from scanners and devices, ensuring compliant, dependable, and secure transfer of imaging data.

RAD 2.4. Provides diagnostic-quality viewing capabilities, including multi-planar reconstruction (MPR), cine playback, and advanced measurement tools.

RAD 2.5. Supports hanging protocols, both system-defined and user-customizable.

RAD 3. Reporting, Workflow, and Tools

RAD 3.1. Complies with DICOM Structed Reporting and modality worklists.

RAD 3.2. Supports metadata-based search and retrieval by patient ID, modality, study type, or diagnosis.

RAD 3.3. Supports configurable retention, deletion, and archival policies, defined by modality, study type, patient record age, or regulatory requirements, and enables system administrators to manage the removal or long-term storage of imaging data accordingly.

RAD 4. Standards And Interoperabilty Requirements

RAD 4.1 Supports standards based interoperability required for exchanging orders, results, images, reports, and clinical data with enterprise Electronic Health Record (EHR) systems and Radiology Information Systems (RIS).

RAD 4.2 Supports all relevant IHE Radiology integration profiles, including Scheduled Workflow (SWF), Patient Information Reconciliation (PIR), Evidence Documents (ED), Key Image Notes (KIN), and Cross Enterprise Document Sharing for Imaging (XDS I), to ensure accurate, automated, and consistent workflow interoperability across radiology acquisition, interpretation, and reporting systems.

RAD 4.3 Provides DICOM Conformance Statements covering all DICOM functions, including support for CT, MR, US, XA, RF, MG, DX, CR, PET, SPECT, multi frame images, and DICOM Encapsulated PDF.

RAD 4.4 Supports HL7 v2.x messaging, including ORM, ORU, ADT, and SIU transactions, to enable standards based order management, results reporting, and scheduling interoperability with RIS and enterprise EHR systems.

RAD 4.5 Supports DICOM Modality Worklist (MWL), Modality Performed Procedure Step (MPPS), and Storage Commitment to ensure accurate, automated workflow interoperability across all radiology modalities and acquisition systems.

RAD 4.6 Supports DICOM Structured Reporting (SR) for radiology measurements, dose reporting, CAD outputs, and quantitative imaging data, including Radiation Dose Structured Reports (RDSR) and Breast Imaging Structured Reporting (BI RADS SR).

RAD 4.7 Supports interoperability with radiology modalities, advanced visualization systems, AI analysis engines, and reporting platforms through standards based interfaces (DICOM, HL7, FHIR, or vendor neutral APIs), ensuring consistent metadata, patient identifiers, and study level attributes.

RAD 4.8 Supports ingestion and retrieval of multi modality radiology datasets, including hybrid imaging (PET/CT, SPECT/CT), multi series MR, multi frame US, and tomosynthesis, using standards based DICOM objects to ensure cross system compatibility and accurate longitudinal comparison.

RAD 4.9. For all Department of Veterans Affairs (VA) delivery orders, the system and associated interfaces shall comply with all VA HL7 implementation guidelines applicable to the designated deployment site(s). The vendor shall be listed on the VA-approved HL7 Interface Vendor List prior to contract award or initiation of HL7-related integration activities. (Reference: https://www.va.gov/imaging/HL7.asp). The vendor shall provide verification of its inclusion on the VA-approved HL7 list upon request. If the vendor is not currently listed, the vendor shall obtain VA HL7 approval before any HL7 messaging, integration, or data exchange work begins.

RAD 5. Security and Compliance Requirements

RAD 5.1 Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

RAD 5.2 Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

RAD 5.3 Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

RAD 5.4 Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools

RAD 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

RAD 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

RAD 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

RAD 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

RAD 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

RAD 6. System Performance and Availability Requirements

RAD 6.1 Provides rapid image acquisition, rendering, and playback with low latency to support real-time clinical decision-making.

RAD 6.2 Supports scalable performance to accommodate increasing imaging volumes, concurrent users, and expanding clinical applications without degradation.

RAD 6.3 Enables efficient access to archived radiology studies (including diagnostic images, prior exams and associated reports), to support clinical review, comparison and ongoing imaging workflows.

RAD 6.4 Optimizes performance across diverse environments including mobile, tablet, workstation, and telehealth devices.

RAD 6.5 Includes performance monitoring dashboards and analytics for system health, response times, throughput, and usage patterns.

RAD 6.6 Provides seamless, automated failover capabilities that transition operations to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity.

RAD 6.7 Implements a high-availability system architecture and disaster recovery design that ensures uninterrupted clinical operations across outpatient clinics, hospitals, and telehealth environments, delivering a minimum of 99.9% system uptime.

RAD 6.8. Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

RAD 6.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms to ensure ongoing operational readiness. All test results shall be logged and made available for audit and compliance review.

RAD 7. Augmented Intelligence (AI) Requirements

RAD 7.1. Provides AI-assisted detection and triage for high priority radiologic findings including stroke, lung nodules, fractures.

RAD 7.2. Supports automated quantitative measurements such as lesion size, volumetrics, and perfusion-related metrics.

RAD 7.3. Provides real-time acquisition guidance and image quality feedback at the point of capture.

RAD 7.4. Integrates AI generated findings, measurements, and annotations directly into structured reporting workflows.

RAD 7.5. Provides predictive analytics to support clinical risk stratification and treatment planning.

RAD 7.6. Ensures explainable AI outputs, including confidence scores, overlays, and traceable rationale.

RAD 7.7. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

RAD 7.8 Stores AI-generated artifacts (segmentations, overlays, derived images, structured findings) using open standards-based formats with full provenance tracking.

SOW - Sleep Lab

The vendor shall provide a fully integrated Sleep Laboratory PACS solution that supports comprehensive sleep medicine workflows, including diagnostic evaluation, therapeutic monitoring, and research applications. The system shall encompass all essential components, software, licensing, and associated support services, to deliver a robust data and imaging management platform specifically optimized for sleep studies and polysomnography.

SLAB 1. General System Requirements.

SLAB 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

SLAB 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

SLAB 1.3. Utilizes vendor-neutral architecture and fully comply with interoperability standards, including DICOM (for waveform and video data), HL7 (for clinical messaging), and FHIR (for RESTful data exchange), to ensure seamless integration with sleep diagnostic systems, EHR platforms, and enterprise archives.

SLAB 1.4. Provides scalable infrastructure to accommodate increasing volumes of sleep studies, expanded service offerings, and multi-site deployments across networked facilities.

SLAB 1.5. Incorporates a high-availability architecture with automated failover and comprehensive disaster recovery capabilities to ensure uninterrupted clinical operations and delivers 99.9% system uptime to support continuous access across outpatient clinics, hospitals, and tele- health environments.

SLAB 1.6. Supports integration with diagnostic algorithms for sleep staging, event detection (e.g., apneas, hypopneas, arousals), and treatment response monitoring, enabling advanced clinical decision support and longitudinal patient tracking.

SLAB 2: Imaging Modality Support Requirements

SLAB 2.1. Receive, process, and archive high-resolution sleep study data and associated imaging, including full-night polysomnography (PSG), Home Sleep Apnea Testing (HSAT), actigraphy, Multiple Sleep Latency Tests (MSLT), Maintenance of Wakefulness Tests (MWT), and synchronized video/audio recordings.

SLAB 2.2. Supports multi-channel waveform data visualization, synchronized video playback, and overlay of physiological signals to enable comprehensive review and analysis of sleep studies.

SLAB 2.3. Supports standardized data formats including European Data Format (EDF), DICOM Waveform, and HL7 Clinical Document Architecture (CDA), ensuring interoperability with sleep diagnostic systems and enterprise health IT platforms.

SLAB 3. Reporting, Workflow, and Tools Requirements

SLAB 3.1. Provides structured reporting templates for adult and pediatric sleep studies, aligned with American Academy of Sleep Medicine (AASM) standards.

SLAB 3.2. Includes tools for tagging sleep-related events such as apneas, hypopneas, arousals, and periodic limb movements (PLMs), as well as capabilities for annotating and comparing sleep studies across multiple timepoints.

SLAB 3.3. Customizable workflow management tools, including study assignment, status tracking, and turnaround time monitoring, with support for role-based task allocation and performance analytics.

SLAB 3.4. Enables longitudinal tracking of patient sleep patterns and outcomes, supporting trend visualization and outcome-based reporting across multiple studies.

SLAB 3.5. Supports secure multidisciplinary collaboration, including remote consultations and encrypted data exchange with referring providers, specialists, and care teams.

SLAB 3.6. Includes integration with voice recognition and/or natural language processing (NLP) platforms to streamline report generation and enhance documentation efficiency.

SLAB 3.7. Includes manual sleep stage scoring tools, allowing technicians to annotate and validate sleep stages in accordance with clinical protocols.

SLAB 4. Image Display and Analysis Requirements

SLAB 4.1. Supports multi-channel waveform display with synchronized video playback to facilitate comprehensive review of sleep studies.

SLAB 4.2. Includes trend analysis tools for evaluating changes in sleep architecture, respiratory patterns, and event frequency over time.

SLAB 4.3. Provides customizable display layouts, allowing users to configure channel views, overlays, and annotation panels based on clinical preferences.

SLAB 5. Security and Compliance Requirements

SLAB 5.1. Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

SLAB 5.2. Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

SLAB 5.3. Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

SLAB 5.4. Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools.

SLAB 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

SLAB 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

SLAB 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

SLAB 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

SLAB 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

SLAB 6. Interoperability Requirements

SLAB 6.1 Supports standards-based interoperability required for exchanging sleep study orders, results, waveforms, signals, scored events, reports, images, videos, and clinical documentation with enterprise Electronic Health Record (EHR) systems.

SLAB 6.2 Supports all relevant IHE profiles for sleep medicine and enterprise imaging, including Scheduled Workflow (SWF), Evidence Documents (ED), Cross-Enterprise Document Sharing (XDS/XDS-I), and any applicable IHE Patient Care Device (PCD) profiles to ensure accurate, automated, and consistent workflow interoperability across sleep study acquisition, scoring, reporting, and documentation systems.

SLAB 6.3 Provide comprehensive DICOM Conformance Statements covering all DICOM functions, including support for DICOM Waveform Storage (e.g., polysomnography waveforms), DICOM Encapsulated Documents (PDF), DICOM Secondary Capture, and DICOM Video where applicable.

SLAB 6.4 Supports HL7 v2.x messaging, including ORM, ORU, ADT, and SIU transactions, to enable standards-based order management, results reporting, patient movement updates, and scheduling interoperability with enterprise EHR systems and sleep lab scheduling systems.

SLAB 6.5 Supports DICOM Waveform Storage (e.g., polysomnography, EEG, EOG, EMG, ECG), DICOM Image Storage for still captures, and DICOM Video Storage where applicable, ensuring consistent, standards-based ingestion and retrieval of sleep study data from all major PSG acquisition systems.

SLAB 6.6 Supports HL7 or FHIR-based exchange of structured sleep study documentation, including scored events, sleep stages, respiratory events, arousal indices, impressions, and coded terminology (e.g., SNOMED CT, LOINC), enabling seamless integration with the EHR and downstream analytics or population health systems.

SLAB 6.7 Supports interoperability with sleep study acquisition systems, scoring software, bedside devices, and waveform capture systems through standards-based interfaces (DICOM, HL7, FHIR, or vendor-neutral APIs), ensuring consistent metadata, timestamps, channel labels, and patient identifiers across all captured content.

SLAB 7. System Performance and Availability Requirements

SLAB 7.1 Provides rapid acquisition, rendering, and playback of sleep study data (including polysomnography (PSG), home sleep apnea testing (HSAT), multi-channel physiologic waveforms, respiratory events, and video

recordings) with low latency and smooth visualization to support timely scoring, interpretation, and clinical assessment.

SLAB 7.2 Supports scalable performance to accommodate increasing volumes of sleep studies, high-density multi-channel datasets, concurrent scoring sessions, and expanding diagnostic applications without degradation in responsiveness or waveform rendering quality.

SLAB 7.3 Enables efficient access to archived studies (e.g., PSG, HSAT, CPAP titration studies, and longitudinal sleep assessments), to support comparative review, treatment response evaluation, and continuity of care.

SLAB 7.4 Optimizes performance across sleep-medicine environments (e.g. scoring workstations, physician review consoles, mobile consultation devices, tablets, and tele-sleep platforms), ensuring consistent waveform clarity, responsive navigation, synchronized video playback, and accurate display of respiratory and neurologic parameters.

SLAB 7.5 Includes performance monitoring dashboards and analytics tailored to sleep medicine workflows, providing visibility into system health, waveform rendering performance, response times, dataset throughput, and usage patterns across sleep labs, clinics, and tele-sleep services.

SLAB 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to sleep study data during active scoring, interpretation, and clinical review.

SLAB 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous sleep-medicine clinical operations, (including PSG acquisition, waveform review, scoring workflows, and reporting) across single-site and multi-facility sleep programs, delivering a minimum of 99.9% system uptime.

SLAB 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting sleep study acquisition, waveform rendering, video playback, or data retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

SLAB 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to sleep-medicine workflows, including PSG dataset retrieval, synchronized video access, waveform continuity, and scoring tool availability. All test results shall be logged and made available for audit and compliance review.

SLAB 8. Augmented Intelligence (AI) Requirements

SLAB 8.1. Includes integrated AI tools to assist with sleep stage scoring, respiratory event detection (e.g., apneas, hypopneas, arousals), and periodic limb movement identification, in accordance with AASM scoring guidelines.

SLAB 8.2. Supports automated detection and classification of sleep disorders such as obstructive sleep apnea (OSA), central sleep apnea, Restless Legs Syndrome (RLS), insomnia, and narcolepsy, with configurable thresholds and diagnostic criteria.

SLAB 8.3. AI-generated summaries, alerts, and annotations shall be available for technician and clinician review, with visual indicators and contextual explanations to support interpretation and validation.

SLAB 8.4. Provides confidence scoring and explainable rationale for all AI-generated outputs, including traceable logic and reference to waveform or video evidence.

SLAB 8.5. Mechanisms are in place to ensure human oversight of AI-assisted interpretations, including manual review, override capabilities, and audit logging of decisions.

SLAB 8.6. Supports customization based on institutional protocols, scoring preferences, and workflow configurations, allowing adaptation to adult, pediatric, and research environments.

SLAB 8.7. Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

SLAB 8.8 Stores AI-generated artifacts (segmentations, overlays, derived images, structured findings) using open standards-based formats with full provenance tracking.

SOW - Veterinary

The vendor shall provide a comprehensive Veterinary Pathology Picture Archiving and Communication System (PACS) designed to support advanced digital pathology workflows in veterinary medicine. The Veterinary PACS shall include all necessary components, software, licensing, and incidental support services, to deliver a fully integrated data and imaging management platform.

VET 1. General System Requirements.

VET 1.1. The system shall integrate with and support bi-directional data exchange with Department of Defense (DoD) and Veterans Affairs (VA) Electronic Health Record (EHR) platforms, Radiology Information Systems (RIS), and other imaging information systems, enabling complete and continuous clinical workflows.

VET 1.2. The system shall interface with current enterprise-approved Vendor Neutral Archives (VNAs) in accordance with the open interoperability standards (DICOM, DICOMweb, and HL7/FHIR) and applicable IHE integration profiles defined in the General Statement of Work to ensure long-term accessibility and retention of all diagnostic data without requiring proprietary middleware.

VET 1.3. Utilizes vendor-neutral architecture and comply with interoperability standards including DICOM for imaging data, HL7 for clinical messaging, and FHIR for RESTful data exchange.

VET 1.4. Scalable to support increasing veterinary imaging volumes across diverse species, expanding diagnostic services such as radiography, ultrasound, CT, MRI, and endoscopy, and multi-site deployments across networked veterinary clinics, hospitals, and specialty centers.

VET 1.5. Incorporates a high-availability architecture with automated failover and comprehensive disaster recovery capabilities to ensure uninterrupted clinical operations and delivers 99.9% system uptime to support continuous access across outpatient clinics, hospitals, and tele health environments.

VET 1.6. Offers tiered storage options with support for lossless compression and metadata indexing to optimize performance and retrieval efficiency.

VET 2. Imaging Modality Support Requirements.

VET 2.1. Securely acquire and archive images from a variety of imaging modalities, including Digital Radiography (DR), Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Ultrasound, and Endoscopy.

VET 2.2. Support non-DICOM image acquisition by allowing the import of images from scanners, cameras and other external sources, with the ability to convert them into DICOM format and compatibility with common image formats such as JPEG, TIFF, PNG, and BMP

VET 2.3. Provide support for archive slide imaging (or WSI), histopathology, cytology, and molecular diagnostics across a wide range of animal species and clinical scenarios.

VET 2.4. Provide support for advanced MRI techniques such as diffusion, perfusion, and spectroscopy.

VET 2.5. The system shall support full compliance with DICOM SOP Classes and standardized DICOM image formats, including Structured Reporting (DICOM SR), ensuring that all relevant DICOM objects and reports can be generated, stored, transmitted, and interpreted in accordance with the DICOM standard.

VET 3. Reporting, Workflow, and Tools Requirements.

VET 3.1. Provide structured reporting templates specifically designed for veterinary radiology, using appropriate findings and terminology.

VET 3.2. Provide tools for tagging, annotating, and comparing veterinary images over time.

VET 3.3. Provide specialized image viewing tools tailored to the anatomy and physiology of various animal species, including features such as zoom, pan, rotate, measurement tools (e.g., distance, area), windowing and leveling adjustments, multi-planar reconstruction (MPR) for CT and MRI images, and 3D rendering.

VET 3.4. Provide customizable workflow management tools (e.g. study assignment, status tracking, turnaround monitoring).

VET 3.5. Support protocols for large animals, including equine radiography.

VET 3.6. Support secure multidisciplinary collaboration, remote veterinary consultations, and data exchange with referring providers and specialists.

VET 3.7. Integrate with voice recognition or natural language processing platforms.

VET 4. Image Display and Analysis Requirements.

VET 4.1. Support multi-planar reconstruction (MPR) for CT and MRI

VET 4.2. Support 3D rendering and volume visualization.

VET 4.3. Display fusion images for PET/CT and SPECT/CT.

VET 4.4. Include visualization techniques such as maximum intensity projection and minimum intensity projection

VET 5. Security and Compliance Requirements.

VET 5.1. Implements role-based user authentication and authorization to ensure secure, least-privilege access to all imaging data and system functions.

VET 5.2. Maintains comprehensive audit trails capturing user activity, system access, configuration changes, and data modifications, supporting compliance review and forensic analysis.

VET 5.3. Encrypts all protected health information (PHI) at rest and in transit using industry-standard protocols (e.g., AES-256 for storage, TLS 1.2 or higher for transmission).

VET 5.4 Complies with all applicable privacy and security regulations, including: HIPAA (Health Insurance Portability and Accountability Act); GDPR (General Data Protection Regulation) for facilities handling EU patient data; and FDA regulations applicable to clinical decision support, imaging software, and AI-enabled tools

VET 5.5 Compliance with any additional specialty-specific guidelines required by the implementing organization (e.g., ACR, AASM, ADA, ACC), without limiting general PACS functionality.

VET 5.6 Provides configurable retention, archival, and purge policies that allow institutions to define storage durations and deletion schedules in accordance with legal, regulatory, and clinical requirements.

VET 5.7 Preserves all associated metadata (DICOM and non-DICOM) and ensures data integrity through validation, checksums, and error-detection mechanisms.

VET 5.8 Provides secure mechanisms for sharing images and reports with external facilities, including encrypted transmission, controlled access, and full audit logging.

VET 5.9 Supports secure data exchange using industry standards such as DICOM, HL7, and FHIR, ensuring interoperability with enterprise EHRs, VNAs, and external imaging systems.

VET 6. Interoperability Requirements

VET 6.1 Supports standards-based interoperability required for exchanging imaging orders, results, diagnostic images, videos, procedure documentation, and clinical data with veterinary practice management systems (PIMS), enterprise Electronic Medical Record (EMR) systems, and multi-site hospital networks.

VET 6.2 Supports all relevant IHE Radiology and enterprise imaging integration profiles, including Scheduled Workflow (SWF), Patient Information Reconciliation (PIR), Evidence Documents (ED), and Cross-Enterprise Document Sharing (XDS/XDS-I), ensuring accurate, automated, and consistent workflow interoperability across veterinary imaging, reporting, and documentation systems.

VET 6.3 Provides comprehensive DICOM Conformance Statements covering all DICOM functions of the proposed Veterinary PACS solution, including support for DICOM Image Storage (CR, DR, CT, MR, US), DICOM Video, DICOM Encapsulated Documents (PDF), and DICOM Secondary Capture, with explicit documentation of species-specific metadata handling.

VET 6.4 Supports HL7 v2.x messaging, including ORM, ORU, ADT, and SIU transactions, to enable standards-based order management, results reporting, patient registration, and scheduling interoperability with veterinary PIMS/EMR systems and multi-modality imaging environments.

VET 6.5 Supports DICOM Image and Video Storage for all major veterinary imaging modalities—including radiography, ultrasound, CT, MRI, fluoroscopy, endoscopy, and dental imaging—ensuring consistent, standards-based ingestion and retrieval of imaging content from diverse veterinary equipment vendors.

VET 6.6 Supports HL7 or FHIR-based exchange of structured diagnostic reports, procedure documentation, and coded terminology (e.g., SNOMED CT Veterinary Extension, LOINC, species/breed coding), enabling seamless integration with PIMS/EMR systems and downstream analytics, research, or population health platforms.

VET 6.7Supports interoperability with veterinary imaging devices, modality worklist providers, reporting systems, and acquisition software through standards-based interfaces (DICOM, HL7, FHIR, or vendor-neutral APIs), ensuring consistent metadata, timestamps, species/breed identifiers, and patient/owner information across all captured content.

VET 7. System Performance and Availability Requirements

VET 7.1 Provides rapid acquisition, rendering, and playback of veterinary imaging modalities, (including radiography, ultrasound, CT, MRI, fluoroscopy, endoscopy, and dental imaging), with low latency and smooth visualization to support timely diagnostic interpretation across diverse species and clinical scenarios.

VET 7.2 Supports scalable performance to accommodate increasing volumes of veterinary studies, multi-modality datasets, concurrent users across treatment areas, and expanding imaging applications without degradation in responsiveness or rendering quality.

VET 7.3 Enables efficient access to archived studies (e.g., radiographs, ultrasound series, CT/MRI datasets, dental images, and endoscopic recordings), to support comparative review, longitudinal monitoring, and continuity of care across species and practice types.

VET 7.4 Optimizes performance across veterinary-specific environments including exam-room workstations, treatment-area consoles, mobile devices, tablets, surgical suites, and tele-consultation platforms, ensuring consistent image clarity, responsive navigation, and accurate display of measurements and annotations.

VET 7.5 Includes performance monitoring dashboards and analytics tailored to veterinary workflows, providing visibility into system health, rendering performance, response times, dataset throughput, and usage patterns.

VET 7.6 Provides seamless, automated failover to redundant or backup system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to veterinary imaging during active examinations, surgical procedures, and emergency care.

VET 7.7 Implements a high-availability architecture and disaster recovery design that ensures continuous veterinary clinical operations—including image acquisition, review, surgical planning, and reporting—across single-site and multi-location practices, delivering a minimum of 99.9% system uptime.

VET 7.8 Includes integrated monitoring, alerting, and fault-detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting veterinary image acquisition, rendering, or retrieval. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

VET 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to veterinary workflows, including radiograph retrieval, ultrasound series access, CT/MRI dataset continuity, and dental imaging availability. All test results shall be logged and made available for audit and compliance review.

VET 8. Augmented Intelligence Requirements

VET 8.1 Integrates with AI tools capable of detecting common veterinary radiographic findings across major species (E.G. canine, feline, equine).

VET 8.2 Supports AI-driven species identification and automatic body-region classification.

VET 8.3 Supports AI-generated measurements such as Vertebral Heart Score (VHS) and other species-appropriate metrics.

VET 8.4 Stores and displays AI outputs, including annotations, overlays, and structured findings, within the PACS viewer and reporting workflow.

VET 8.5 Ensures that deployed AI models operate as fixed, non-learning systems in the clinical environment, while supporting structured user feedback capture for off-site model retraining. Any updated AI models must undergo external validation, regulatory review, and formal approval before deployment to replace the existing fixed model.

VET 8.6 Maintains auditable logs of AI usage, model versions, and confidence scores.

VET 8.7 Stores AI-generated artifacts (segmentations, overlays, derived images, structured findings) using open standards-based formats with full provenance tracking.

SOW - Vendor Neutral Archive

The vendor shall provide an enterprise-grade Vendor Neutral Archive (VNA) that utilizes standards-based, vendor-agnostic storage, normalization, lifecycle management, and cross-system exchange of imaging and related clinical data across all specialties. The VNA shall function as the enterprise imaging repository and must include all software, components, licensing, and support services necessary to ensure long-term accessibility, interoperability, and governance of imaging objects and associated metadata. The solution shall fully comply with the minimum VNA requirements defined below, including support for DICOM and non-DICOM ingestion, metadata normalization, tiered storage and lifecycle management, cross-enterprise image exchange, security and audit controls, high-availability performance, and standards-based storage of AI-generated artifacts.

VNA 1. General System Requirements.

VNA 1.1 The system shall provide a vendor neutral, standards based architecture supporting DICOM, DICOMweb, HL7, and FHIR for the exchange, storage, and retrieval of imaging and related clinical data.

VNA 1.2 The system shall support bidirectional interoperability with enterprise EHR platforms, RIS, PACS, and DoD/VA approved imaging systems for demographics, orders, metadata, and study retrieval.

VNA 1.3 The system shall provide an enterprise-wide repository that ensures the long-term accessibility, integrity, and future-readiness of imaging and diagnostic records across all clinical specialties by meeting the following requirements:

VNA 1.3.1 Standards-Based Exchange & Ingestion: The system shall support secure, standards-based interoperability for the ingest, archival, retrieval, and exchange of imaging and diagnostic data across all enterprise specialties and approved imaging systems using open, industry-recognized standards (including DICOM, DICOMweb, and HL7/FHIR).

VNA 1.3.2 Complete Record & Metadata Integrity: The system shall preserve all associated DICOM and non-DICOM metadata during the archival, normalization, exchange, and retrieval processes, ensuring the long-term clinical accessibility, diagnostic fidelity, and complete integrity of the patient record.

VNA 1.3.3 Successor Archive Migration & Federation: The system shall support standards-based federation and lossless data extraction/migration to other enterprise-approved repositories or successor archives without proprietary data conversion fees or vendor-imposed exit restrictions.

VNA 1.3.4 Expandability for Emerging Standards: The system shall provide the modular interfaces and expandability necessary to accommodate evolving Government requirements and emerging consensus interoperability standards (such as subsequent revisions published by the DICOM Standards Committee, HL7 International, and IHE) without requiring core architectural redesign.

VNA 2. Imaging Modality Support Requirements.

VNA 2.1 The system shall store imaging objects and related documents from all specialties using standards compliant formats (e.g., DICOM, JPEG, PDF, MPEG 4).

VNA 2.2 The system shall normalize and standardize metadata, including DICOM header correction, tag normalization, identifier harmonization, and enforcement of enterprise naming conventions.

VNA 2.3 The system shall support non DICOM ingestion (e.g., photos, videos, PDFs, waveforms) with appropriate metadata mapping.

VNA 2.4 The system shall maintain robust metadata indexing to enable efficient search and retrieval based on patient demographics, modality, study attributes, or other enterprise defined metadata.

VNA 2.5 The system shall support linkage of related studies and longitudinal patient records across episodes of care.

VNA 3. Reporting, Workflow, and Tools Requirements

VNA 3.1 The system shall provide tiered storage management, including fast storage, object storage, and deep archive, with automated migration between tiers.

VNA 3.2 The system shall enforce configurable retention, deletion, and de identification policies aligned with regulatory and clinical requirements.

VNA 3.3 The system shall support lossless compression and storage optimization while preserving diagnostic integrity.

VNA 3.4 The system shall enable seamless data migration to new storage platforms without downtime or data loss.

VNA 4. Image Display and Analysis Requirements

VNA 4.1 The system shall support cross enterprise image exchange, including XDS I registry/repository functions and FHIR based image access.

VNA 4.2 The system shall enable secure retrieval of imaging studies by any authorized PACS, viewer, or clinical system.

VNA 4.3 The system shall support mobile and point of care access through standards based APIs without requiring proprietary viewers.

VNA 5. Compliance and Security Requirements

VNA 5.1. The system shall comply with applicable regulatory frameworks governing imaging data and PHI, including HIPAA, GDPR, and DoD/VA security requirements.

VNA 5.2 The system shall provide comprehensive audit logging, access controls, and data provenance tracking for all stored and exchanged objects.

VNA 5.3 The system shall ensure encrypted transmission and secure access for all internal and external data exchanges.

VNA 6. Interoperability Requirements

VNA 6.1 Supports standards-based interoperability required for exchanging, storing, retrieving, and managing imaging and clinical objects, including DICOM, non DICOM, documents, and multimedia, across all enterprise imaging systems and the Electronic Health Record (EHR).

VNA 6.2 Supports all relevant IHE Enterprise Imaging integration profiles, including XDS, XDS I, XCA I, IOCM (Image Object Change Management), and Evidence Documents (ED), to ensure consistent, standards-based interoperability across multi department imaging workflows.

VNA 6.3 Provides comprehensive DICOM Conformance Statements covering all DICOM functions, including support for DICOM Storage, Query/Retrieve, Storage Commitment, Modality Worklist (MWL), and DICOMweb services (WADO RS, QIDO RS, STOW RS).

VNA 6.4 Supports HL7 v2.x messaging, including ORM, ORU, ADT, and SIU transactions, to enable standards-based order, results, and scheduling interoperability with enterprise EHR systems, PACS, and specialty imaging platforms.

VNA 6.5 Supports ingestion, storage, and retrieval of non DICOM objects, including JPEG, PNG, TIFF, PDF, MPEG 4, WAV, DOCX, and other clinical media, using standards-based encapsulation (DICOM Encapsulated Document, DICOM Encapsulated Video) or vendor neutral APIs.

VNA 6.6 Supports DICOMweb (WADO RS, QIDO RS, STOW RS) for modern, standards based RESTful interoperability with enterprise viewers, PACS, mobile applications, and cloud-based imaging systems.

VNA 6.7 Supports metadata normalization, mapping, and reconciliation across all connected imaging systems, including PACS, modalities, specialty systems, and EHR platforms, to ensure consistent patient identifiers, study metadata, and enterprise wide searchability.

VNA 6.8 Supports Cross Enterprise Document Sharing (XDS/XDS I) for multi facility and regional image exchange, enabling standards-based sharing of imaging studies and clinical documents across disparate health systems.

VNA 6.9 Supports interoperability with PACS, enterprise viewers, AI analysis engines, and specialty imaging systems through standards-based interfaces (DICOM, HL7, FHIR, DICOMweb, XDS, or vendor neutral APIs), ensuring consistent access, metadata integrity, and lifecycle management across the enterprise.

VNA 7. VNA Performance and Availability Requirements

VNA 7.1 Provides rapid ingestion, indexing, retrieval, and rendering of enterprise imaging objects (including DICOM studies, non DICOM clinical media, documents, waveforms, and metadata) with low latency to support timely clinical access across all departments and care settings.

VNA 7.2 Supports scalable performance to accommodate increasing volumes of multimodality imaging, large scale archival datasets, concurrent enterprise users, and expanding departmental integrations without degradation in responsiveness, ingestion speed, or retrieval performance.

VNA 7.3 Enables efficient access to archived studies and non-imaging objects (e.g., radiology studies, cardiology loops, pathology slides, dermatology photos, endoscopy videos, POCUS clips, and clinical documents), support longitudinal review, multidisciplinary collaboration, and enterprise-wide clinical decision making.

VNA 7.4 Optimizes performance across diverse environments (including PACS viewers, EHR systems, mobile devices, specialty workstations, telehealth platforms, and third-party applications, ensuring consistent access speed, metadata integrity), and rendering quality regardless of originating system or device.

VNA 7.5 Includes performance monitoring dashboards and analytics tailored to enterprise imaging workflows, providing visibility into system health, ingestion and retrieval performance, storage utilization, metadata indexing behavior, and usage patterns across all connected clinical systems.

VNA 7.6 Provides seamless, automated failover to redundant or geographically distributed system resources during hardware, software, or network failures. Failover shall occur without user intervention and without loss of data integrity, ensuring uninterrupted access to imaging and clinical objects across the enterprise.

VNA 7.7 Implements a high availability architecture and disaster recovery design that ensures continuous enterprise imaging operations (including ingestion, storage, retrieval, lifecycle management, and interoperability services), across single site, multi-site, and regional networks, delivering a minimum of 99.9% system uptime.

VNA 7.8 Includes integrated monitoring, alerting, and fault detection mechanisms capable of identifying failures, degraded performance, or service interruptions affecting ingestion pipelines, metadata services, storage tiers, or retrieval workflows. Upon detection, the system shall automatically initiate predefined recovery procedures without manual operator action.

VNA 7.9 Performs automatic, periodic validation and testing of failover and disaster recovery mechanisms specific to enterprise imaging workflows, including DICOM and non-DICOM ingestion, metadata indexing, cross-system retrieval, and lifecycle management continuity. All test results shall be logged and made available for audit and compliance review.

VNA 8. AI Object Storage & Metadata Handling

VNA 8.1 The system shall store AI generated artifacts (e.g., segmentations, overlays, derived images, structured findings) using standards-based formats with full provenance tracking.

VNA 8.2 The system shall ingest and index AI generated metadata to support enterprise search, analytics, and routing.

VNA 8.3 The system shall maintain auditable logs of AI-related metadata, including model identifiers, timestamps, and confidence scores, without executing or managing AI models.

VNA 8.4 The system shall ensure compliance with regulatory requirements governing the storage and handling of AI generated clinical data.

SOW Appendix 1 – DICOM Requirements

1.1. DIN-PACS Modality and DICOM Interface Requirements.

1.1.1. Introduction: This Appendix outlines the DICOM conformance requirements for the DIN-PACS system. The specification is written from an "outside perspective" into the DIN-PACS system—i.e., based on the functions that must be provided via the DICOM interface, viewed from the standpoint of connected devices.

1.1.2. General Requirements: The DIN-PACS interface shall conform to the DICOM Standard (available at https://www.medical.nema.org) in effect six months prior to the issuance of the site-specific delivery order. Additionally, the interface shall meet the specific requirements defined below, upon request. The vendor shall submit DICOM conformance statements for the proposed DIN-PACS system, compliant with the format described in Part PS 3.2 of the DICOM standard. The vendor must support Explicit Value Representation (VR) Presentation Syntax. Note: The Government may request the vendor's IHE Statement and/or DICOM Conformance Standard at any time to verify compliance with applicable standards.

1.1.3. DIN-PACS Modality and DICOM Interface Requirements: The DIN-PACS system shall provide a Modality Worklist to the modality. Schedule and required patient demographic information shall be provided so that operators at the modality do not need to re-enter this data.

1.2. Level of Conformance

1.2.1 The DIN-PACS shall provide full conformance (Level 2) with respect to the required Storage Classes. All Type 1, 2, and 3 attributes that are communicated shall be stored and accessible. Coercion is permitted for Patient ID, Study Instance UID, and Series Instance UID to synchronize the DIN-PACS database with the Hospital Information System (HIS). Additionally, the DIN-PACS must support two scenarios where images are sent without complete identification:

(a) A study has not been entered in the Radiology Information System (RIS) prior to the exam, and the modality cannot retrieve the information from the DIN-PACS. Patient information is entered at the modality, and a Study Instance UID is generated by the modality. The DIN-PACS must be able to match this study later with the Study ID generated by the RIS after image transfer.

(b) Patient information is unknown (e.g., trauma cases). In such cases, patient information and Study ID must be linked to the images in the DIN-PACS using data entered into the RIS after image transfer.

1.3. Required Attributes

1.3.1. Each modality worklist entry shall contain, at a minimum:

(a) Patient Name;
(b) Patient ID;

(c) Order/Accession Number;
(d) Requested Procedure Description;
(e) Scheduled Station Application Entity; and
(f) Modality or Modalities in Study

1.3.2. Configurable Parameters: All operational parameters that may influence performance and/or Application Entity (AE) behavior shall be configurable. These include:

(a) Number of simultaneous associations
(b) Maximum PDU size
(c) Timeout values
(d) Local AE Titles
(e) Local IP Address and Subnet Mask
(f) Remote AE Title fields
(g) Responding TCP/IP ports and addresses

Upon request, the vendor shall provide a complete list of these parameters, including their configurable value ranges.

1.3.3. Future Standard Extensions: The DIN-PACS vendor shall demonstrate plans to implement future extensions to the DICOM standard. This includes, but is not limited to:

(a) Support for additional Storage, Service-Object Pair (SOP) Classes, using newly defined Information Object Definitions (IODs)
(b) Capability to receive information from the modality via the Performed Procedure Step Service Class

1.3.4. DICOM Data Elements: The DIN-PACS vendor shall conform with Registry of DICOM Data Elements per the DICOM standard. This includes the Registry Standard for DICOM Tags in Table 6-1 (https://dicom.nema.org/medical/dicom/current/output/chtml/part06/chapter_6.html).

1.4. DICOM Modalities

1.4.1. Contractors shall support integration of emerging or new DICOM modalities as they become available.

1.4.2. A detailed description of the image acquisition method shall be provided for each type of image acquisition system. This description shall include:

(a) How correct Patient ID and Study unique identifier (UID) are obtained
(b) How housekeeping functions for DICOM objects (Image Series, Study Components, Study IODs) are managed

1.4.3. The system shall include one or more DICOM Storage Service Class Providers (SCPs) that support all necessary Storage SOP Classes required by the DICOM Storage Service Class Users (SCUs) implemented on each image acquisition system.

1.4.4. The system shall include a DICOM Query/Retrieve SCP/SCU to support imaging modalities, third-party workstations, and foreign archives.

1.4.5. The DICOM Query/Retrieve SCP shall support, at a minimum, the Study Root Query/Retrieve Information Model.

1.4.6. The system shall include a DICOM Modality Worklist Management SCP (DICOM Supplement 10) and support modality worklists.

1.4.7. The system shall include a DICOM Storage Commitment Push Model SCP to accept ownership of identified images.

1.4.8. The system shall include a DICOM Study Component Management SCP to correctly map identified images to Radiology Information System (RIS) ordered studies.

1.4.9. In cases where a procedure is performed without prior RIS registration and no patient information or Study UID is available, the modality shall allow manual entry of patient information and generate its own Study UID. The system shall include an automated mechanism to remap this UID once the RIS order is performed and communicated, thereby correctly associating the images with the appropriate RIS-ordered exam.

1.4.10. Upon request, the vendor shall provide one or more Conformance Statements with the proposal, covering all DICOM functions of the system.

1.4.11. Upon request, the vendor shall provide conformance testing results that validate the system's Conformance Statements.

(End Appendix 1)

SOW Appendix 2 – Contract Data Requirements List (CDRL)

2.1 CDRL Documentation Requirements

The Contractor shall provide, on a site-specific basis as outlined in each delivery order, one or more documentation items (DD Form 1664 for DoD orders and as attachment for VA delivery orders, items AA through AG), when applicable. The specific items required will be identified in the delivery order for each site.

The Government reserves the right to make minor changes to submittal requirements—individually or globally—throughout the contract term. These adjustments may reflect evolving technology or industry standards. If such changes affect the Contractor's preparation costs, they will be negotiated with the contracting officer as needed.

Item	Title
AA	DIN-PACS Operation and Maintenance Data
AB	Extended Installation Plan
AC	Master Components and Parts List
AD	System Security Plan
AE	Quality Control (QC) Plan
AF	Crisis Management Plan
AG	Disaster Recovery Plan

Table 1.1 - Contract Data Requirements List

DATA ITEM DESCRIPTION			Form Approved OMB No. 0704-0188
1. TITLE **DIN-PACS Operation and Maintenance Data**		2. IDENTIFICATION NUMBER **AA**	
3. DESCRIPTION/PURPOSE The Contractor shall submit an DIN-PACS Operation and Maintenance Data Plan for the delivery order.			
4. APPROVAL DATE *(YYMMDD)*	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) DLA Troop Support – Capital Equipment Division	6a. DTIC APPLICABLE	6B. GIDEP APPLICABLE
7. APPLICATION/INTERRELATIONSHIP			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER	

10. PREPARATION INSTRUCTIONS

At a minimum, the contractor shall provide all maintenance and diagnostic software, system administration guides, operating instructions, and maintenance manuals for all DIN-PACS components (hardware, software, and ancillary items), required for successful operation and maintenance.

1. DIN-PACS Equipment Documentation

The Contractor shall provide commercial system administration manuals, operator manuals, and maintenance manuals for the supplied DIN-PACS system and all subsystems. Documentation shall include wiring schematics, parts price lists, installation instructions, inspection procedures and standards, theory of operation, sub-component removal and repair procedures, diagnostic software operation and configuration instructions, testing and troubleshooting procedures, and system maintenance procedures. Copies of document corrections shall be supplied for the life of the system.

2. DIN-PACS Maintenance and Diagnostic Software

The Contractor shall provide DIN-PACS system software with the supplied system, delivering two copies per site—one to remain with the system and one for the facility's biomedical maintenance branch. All software and supporting documentation shall be updated as software upgrades are released.

3. Sub-Component Integration and Testing Requirements

For any CLIN item composed of multiple sub-components (e.g., a workstation with CPU, monitors, network interfaces, software, and storage), the maintenance and diagnostic software documentation must include detailed descriptions of sub-component integration, as well as procedures for system-level and sub-component testing and repair.

11. DISTRIBUTION STATEMENT

As cited in delivery order.

DATA ITEM DESCRIPTION			Form Approved OMB No. 0704-0188
1. TITLE **Extended Installation Plan**		2. IDENTIFICATION NUMBER **AB**	
3. DESCRIPTION/PURPOSE The Contractor shall submit an Extended Installation Plan for the delivery order.			
4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) DLA Troop Support – Capital Equipment Division	6a. DTIC APPLICABLE	6B. GIDEP APPLICABLE
7. APPLICATION/INTERRELATIONSHIP			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER	

10. PREPARATION INSTRUCTIONS

At a minimum, the contractor shall provide a site-specific plan that defines management roles, execution schedules, quality control measures, detailed work requirements.

1. Management Plan

1.1. Project Management

The Contractor shall identify all personnel involved in project management, from senior leadership to the full-time, on-site project manager. For each individual, the Contractor shall provide the name, title, assigned responsibilities, qualifications, email address, and phone number.

1.2. Project Execution

The Contractor shall provide a schedule detailing site preparation, deliveries, and installation activities. The schedule must include provisions for:

A. Storage of tools, equipment, and materials, and subcontractor access to installation site.

B. Actions planned to minimize disruption to traffic and other routine operations, coordinated with the Government on-site representative.

C. The method agreed upon between the Contractor and the Government on-site representative to coordinate the interruption of power and/or other utilities when necessary for installation.

D. The times and procedures agreed upon between the Contractor and the Government on-site representative for work items that may cause excessive noise or structural vibrations (e.g., core-drilling).

E. Acknowledgment of the specific site's normal duty hours.

1.3. Quality Control

The Contractor shall submit a quality control plan covering all work, including subcontractors, to ensure compliance with contract specifications and applicable building and utility codes. The plan shall address the requirement to secure all necessary payment and performance bonds, permits, licenses, and insurance for construction activities. It shall also describe how the Contractor will perform all inspections and tests required by the technical provisions of the contract, supported by an inspection schedule aligned with the project execution timeline and delivery milestones. This schedule shall identify each inspection and test, reference the applicable specifications, standards, or codes, list responsible personnel and their roles, and estimate the time required for each activity.

Additionally, the Contractor shall provide a list of all subcontractors, consultants, and testing laboratories to be used on the project, including a description of the specific maintenance and diagnostic software or work each firm will perform at each site. The plan shall also identify all individuals authorized to sign shop drawings, samples, certificates, and other submittals to verify compliance with contract requirements.

-------Continue Next Page-------

2. Production Plan

2.1. Work Statements

Work statements and associated costs for extended installation efforts must be provided for each task necessary to accomplish site preparation for the DIN-PACS system at each location. The work statements must include descriptive text detailing the required work. Specifically, the work statement(s) shall include descriptions, instructions, standards, specifications, rules, quality requirements, qualifications, limitations, schedules, and requirements for all materials, tools, equipment, labor, procedures, services, construction, and demolition, as applicable. The work statement(s), with costs, shall be prepared using the Construction Specifications Institute (CSI) 50-division format (MASTERFORMAT).

2.2. Work Breakdown Structure (WBS) and Site-Specific Price Breakdown

When deemed necessary by the Contracting Officer—based on task or division scope, complexity, or cost—the Contractor shall submit a Work Breakdown Structure (WBS) as part of the site-specific Production Plan for evaluation. The WBS must be provided upon request for the identified task(s) or division(s). Additionally, a detailed site-specific price breakdown for equipment, installation, and site preparation shall be submitted for each DIN-PACS location.

11. DISTRIBUTION STATEMENT

As cited in delivery order.

DATA ITEM DESCRIPTION			Form Approved OMB No. 0704-0188
1. TITLE Master Component and Parts List		2. IDENTIFICATION NUMBER **AC**	
3. DESCRIPTION/PURPOSE The Contractor shall submit a Master Parts List for the delivery order.			
4. APPROVAL DATE *(YYMMDD)*	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) DLA Troop Support – Capital Equipment Division	6a. DTIC APPLICABLE	6B. GIDEP APPLICABLE
7. APPLICATION/INTERRELATIONSHIP			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER	

10. PREPARATION INSTRUCTIONS

The Contractor shall submit a comprehensive components and parts list for the system. Each item must be identified by manufacturer's name and part number. The list shall include, but is not limited to, the following information:

a. Manufacturer's name
b. Item name
c. Manufacturer's part number
d. Diagram reference
e. Contract CLIN number if applicable for the component
f. Contract CLIN item name if applicable for the component
g. Manufacturer's name of sub-component
h. Item name of sub-component
i. Manufacturer's part number of sub-component
j. Diagram reference of sub-component
k. Number of sub-components per component

IMPORTANT: Items in the master components and parts list must be grouped by function (e.g., workstation) and further organized by room number or physical location to support efficient identification and inspection.

11. DISTRIBUTION STATEMENT

As cited in delivery order.

DATA ITEM DESCRIPTION			Form Approved OMB No. 0704-0188
1. TITLE **System Security Plan**		2. IDENTIFICATION NUMBER **AD**	
3. DESCRIPTION/PURPOSE The Contractor shall submit a system security plan for the delivery order.			
4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) DLA Troop Support – Capital Equipment Division	6a. DTIC APPLICABLE	6B. GIDEP APPLICABLE
7. APPLICATION/INTERRELATIONSHIP			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER	

10. PREPARATION INSTRUCTIONS

The Contractor shall develop and submit a comprehensive System Security Plan (SSP) detailing the safeguards in place to protect all Protected Health Information (PHI) processed, stored, or transmitted by the system. The SSP shall comply with the requirements of DoDI 8510.01, Risk Management Framework (RMF) for DoD IT, the Department of Defense Cyber Security Risk Management Construct (CSRMC), where applicable, and the National Institute of Standards and Technology (NIST) Special Publication 800-37.

At a minimum, the System Security Plan shall include the following elements:

General Description and Purpose

Provide a concise overview (one to three paragraphs) describing the system's primary functions, operational purpose, and the nature of the information it processes.

Required Content

1. A description of the database backup procedures.
2. A description of the database restoration procedures.
3. A description of the procedures used to test database backup and restoration processes.
4. A description of the trusted recovery procedures.
5. A description of the Relational Database Management System (RDBMS) security policies.
6. A description of the testing procedures for RDBMS installations, patches, and updates.
7. A description of the database encryption mechanisms.
8. A description of RDBMS roles and associated privileges.
9. A description of the procedures used to monitor unauthorized changes to the RDBMS, including libraries, related software applications, and configuration files.
10. A description of how inactive RDBMS accounts are monitored and managed.
11. A description of how the integrity of RDBMS data is maintained in a secure state during system initialization, shutdowns, and abort conditions.

11. DISTRIBUTION STATEMENT

As cited in delivery order.

DATA ITEM DESCRIPTION			Form Approved OMB No. 0704-0188
1. TITLE **Quality Control (QC) Plan**		2. IDENTIFICATION NUMBER **AE**	
3. DESCRIPTION/PURPOSE The Contractor shall submit a QC program specific to the delivery order.			
4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) DLA Troop Support – Capital Equipment Division	6a. DTIC APPLICABLE	6B. GIDEP APPLICABLE
7. APPLICATION/INTERRELATIONSHIP			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER	

10. PREPARATION INSTRUCTIONS

The Contractor shall develop and maintain a Quality Control (QC) Plan specific to the DIN-PACS system and tailored to the requirements of each delivery order. The QC Plan shall describe the processes, methods, and controls the Contractor will use to ensure all products and services meet the performance, functional, and technical requirements established by the Government.

DIN-PACS Quality Control (QC) Plan Requirements:

1. Purpose

The quality control (QC) plan shall ensure that all images, workflows, system components, and data consistently meet clinical, technical, and regulatory standards.

2. Procedures

The QC Plan shall describe the procedures used to verify system performance and compliance. At a minimum, procedures shall address software validation, hardware inspection and verification, network connectivity and communication pathway checks, image quality and data integrity verification.

3. Performance Metrics and Standards

The QC Plan shall define measurable performance criteria and identify applicable standards, including but not limited to system uptime and availability, response time and throughput, error rates and defect thresholds, and compliance with DICOM and other applicable standards.

4. Inspection and Testing Schedule

The QC Plan shall include a schedule for routine and event driven QC activities. At a minimum, the plan shall identify the frequency of recurring QC inspections and the QC activities required after system changes, updates, or repairs.

5. Documentation Requirements

The QC Plan shall describe how QC activities will be documented and maintained. Documentation shall include, at a minimum, the date and time of QC activity, the personnel performing the activity, the tests performed and results obtained, and the identified deficiencies and corrective actions taken.

6. Non-Conformance and Corrective Action

The QC Plan shall define procedures for identifying, documenting, and correcting deficiencies. At a minimum, the plan shall include deficiency identification and reporting, corrective action timelines, and re-testing and verification procedures.

7. Reporting Requirements

The QC Plan shall specify all QC reports required by the Government, including their submission frequency, required content, and submission format.

-------Continue Next Page-------

8. Compliance Requirements

The QC Plan shall identify all applicable standards, regulations, and policies governing QC activities, including DICOM standards, cybersecurity and information assurance requirements, and agency specific imaging or IT policies.

11. DISTRIBUTION STATEMENT

As cited in delivery order.

DATA ITEM DESCRIPTION			Form Approved OMB No. 0704-0188
2. TITLE **Crisis Management Plan**		1. IDENTIFICATION NUMBER **AF**	
3. DESCRIPTION/PURPOSE The Contractor shall submit a crisis management plan specific to each delivery order.			
4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) DLA Troop Support – Capital Equipment Division	6a. DTIC APPLICABLE	6B. GIDEP APPLICABLE
7. APPLICATION/INTERRELATIONSHIP			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER	

10. PREPARATION INSTRUCTIONS

The Contractor shall submit a crisis management plan as required for each delivery order to illustrate all steps to be taken by the Contractor to ensure clinical capability in case of a system crisis/shutdown (should include scenarios to cover all critical subsystems as well as the entire system overall).

At a minimum, the Crisis Management Plan shall define all actions, procedures, and contingencies necessary to ensure uninterrupted clinical capability in the event of a system disruption affecting the DIN-PACS.

1. Partial System Failure

The Crisis Management Plan shall provide detailed procedures for maintaining clinical operations during the failure of individual critical subsystems, including but not limited to a single server or hardware component, a specific software module, or a network segment or communication pathway. The plan shall describe interim workflows, mitigation steps, and restoration procedures for each identified subsystem.

2. Total System Failure

The Crisis Management Plan shall provide procedures for responding to a complete DIN-PACS outage, in which the entire system is non-operational. The plan shall include continuity workflows enabling clinical operations to proceed without DIN-PACS, temporary documentation, imaging, and communication processes, and defined steps and responsibilities for system recovery and restoration.

11. DISTRIBUTION STATEMENT

As cited in delivery order.

DATA ITEM DESCRIPTION			Form Approved OMB No. 0704-0188
2. TITLE **Disaster Recovery Plan**		1. IDENTIFICATION NUMBER **AG**	
3. DESCRIPTION/PURPOSE The Contractor shall submit a Disaster Recovery Plan specific to the delivery order.			
4. APPROVAL DATE (YYMMDD)	5. OFFICE OF PRIMARY RESPONSIBILITY (OPR) DLA Troop Support – Capital Equipment Division	6a. DTIC APPLICABLE	6B. GIDEP APPLICABLE
7. APPLICATION/INTERRELATIONSHIP			
8. APPROVAL LIMITATION	9a. APPLICABLE FORMS	9b. AMSC NUMBER	

10. PREPARATION INSTRUCTIONS

At a minimum, this document defines the processes, resources, and responsibilities required to restore system functionality following a disruptive event. The plan shall outline recovery priorities, system dependencies, data restoration procedures, failover operations, and communication protocols to ensure continuity of medical imaging services and preservation of clinical data integrity, and shall describe the recovery procedures, roles, communication protocols, system restoration steps, data recovery methods, and testing requirements relevant to DIN-PACS disaster scenarios.

1. Roles and Responsibilities

The disaster recovery plan shall identify the roles and responsibilities of Contractor and Government personnel involved in disaster recovery operations.

2. System Recovery Priorities

The disaster recovery plan shall provide a description of critical DIN PACS components and recovery priorities, along with the defined Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) that guide restoration efforts.

3. Data Backup and Validation

The disaster recovery plan shall describe data backup schedules, storage locations, and validation procedures necessary to ensure recoverability and data integrity.

4. System Restoration Procedures

The disaster recovery plan shall outline the procedures for system shutdown, failover activation, and full restoration, including the steps required to restore DICOM services, database integrity, and user access.

5. Communication and Escalation

The disaster recovery plan shall define communication and escalation protocols to be followed during outages and throughout the recovery process.

6. Testing and Reporting

The disaster recovery plan shall establish the testing requirements for annual disaster recovery exercises and the post recovery reporting and documentation requirements.

11. DISTRIBUTION STATEMENT

As cited in delivery order.

SOW Appendix 3 – Installation, Extended Installation, Interfaces/Integration

3.1 Equipment Installation

3.1.1. Contractor's Responsibility in Connection with Installation.

3.1.1.1. Contractor and Site Duties for Installation:

For DoD & VA Delivery Orders:
For on-site installations, the offered price for all DIN-PACS solutions under the contract shall include the full cost of installation. Installation consists of assembling, positioning, and mounting all equipment listed in the delivery order, as well as connecting all required cables. The site is responsible for providing all conduit and raceways unless otherwise specified in the delivery order. The Contractor is responsible for supplying and installing all interconnecting wiring and cabling. For cables routed through conduit and raceways, the Contractor shall pull the cables and make all necessary connections. For wiring and cabling not routed through conduit and raceways, the Contractor shall furnish and install the wiring and cabling. Additionally, the Contractor is responsible for installing all junction boxes, wall and ceiling mounts, and support structures that are supplied by the contractor.

For VA Delivery Orders:
Pre-Staging of Equipment: Prior to shipment to VA or facilities, the Contractor shall perform all required pre-staging activities for hardware included in the delivery order. Pre-staging includes unboxing, initial configuration, functional verification, and repacking of equipment for shipment. The Contractor shall maintain all original packaging materials and shall ensure that each hardware item is returned to its original box with the correct serial number, license labels, and any other identifying documentation. The Contractor shall keep all equipment and packaging organized in a manner that enables VA/ Logistics personnel to accurately receive, inventory, and establish property records upon delivery.

3.1.1.2. Contractor Staffing and Performance Obligations: The Contractor shall provide well-qualified field engineers or technicians to perform the installation and conduct all necessary testing. These activities shall commence within 10 days of receiving the Government's notice to proceed. Once installation begins, it shall continue uninterrupted for eight hours per day or until completion, if sooner, aligning with the site's regular working hours. Compliance with this requirement will be demonstrated by the continuous presence of the engineers and/or technicians at the job site during each working day-and documenting progress via email. Installation and testing shall proceed without interruption until it is fully completed. The Contractor is also responsible for transporting the Contractor-provided equipment from the delivery point at the destination to the designated installation area, as well as uncrating the equipment.

3.1.2. Contractor's Responsibility in Connection with Extended Installation:

3.1.2.1. The Government may require extended installation work beyond the scope outlined in Section 3.1.1 above. The costs associated with extended installation are not included in the standard price of the DIN-PACS solution and shall be negotiated separately. These costs must be quoted on a site-specific basis, as defined in the corresponding delivery order.

(A) Extended installation shall, at a minimum, include connecting to existing utilities and furnishings and installing the necessary support structures for the DIN-PACS system.

(B) Extended installation may include, but is not limited to, the provision and installation of power transformers, step-up or step-down transformers, power runs, disconnects, conduit, wiring, structural supports, shielding, and HVAC systems when necessary to support system operations. It may also encompass networking infrastructure required for the routine clinical use of the DIN-PACS system and any related equipment items.

(C) Upon request of the Government, the Contractor shall supply the following:

(1) Preliminary Statement of Work and single-line room drawings: Submission of the Statement of Work will serve as verification that the existing utilities are adequate to support the system(s).

(2) Extended Installation Price Breakdown: A detailed cost breakdown for extended installation shall be provided, specific to each site and delivery order.

3.1.2.2. The Contractor's Extended Installation Statement of Work shall include, at a minimum, the date(s) on which the site survey(s) were conducted, a detailed scope of work outlining the tasks to be performed and the materials to be used, a single-line room drawing, and a total cost statement covering both labor and materials. All cost statements

must be presented in accordance with the Construction Specifications Institute (CSI) 50-Division format (MASTERFORMAT) of standardized divisions. Any site preparation work necessary to ensure a fully functional system—whether or not explicitly identified in the Statement of Work but required for system operation—shall be the responsibility of the Contractor.

3.1.2.3. When extended installation is required, the Contractor shall provide all necessary design plans, labor, materials, and equipment to complete the installation in support of the designated system. The installation shall adhere to nationally recognized trade organization codes and meet, at a minimum, the standards necessary to ensure a safe and functional system.

3.1.2.4. During the site survey(s), the Government point of contact at the installation site(s) shall provide the Contractor, upon request, with a written analysis of the existing and available site power supply and the load-bearing capacity of the floor, ceiling, and walls. Associated drawings shall also be provided if available. The Contractor shall be responsible for furnishing structural support, shielding, and HVAC only as defined in the Statement of Work, provided such provisions are sufficient to fully support the system being installed.

3.1.2.5. Once the Contractor has conducted the site visit(s) and submitted a quote for the extended installation work, they shall not be held responsible for any additional site preparation requirements resulting from Government modifications to the installation site(s) made after the Contractor's visit. However, the Contractor may be requested to submit a revised or supplemental Statement of Work to address any newly required extended installation work.

3.1.3. Drawings and Site Preparation Instructions:

3.1.3.1. For installation and extended installation, the Contractor is responsible for visiting the installation site(s) to assess power and utility requirements, room dimensions, and other physical characteristics necessary for proper system layout. Within 30 calendar days of receiving the delivery order, and if the site requires preparation that includes either construction or infrastructure changes, then the Contractor shall provide the ordering agency or its designee with the following: two complete layout plans, room preparation drawings suitable for developing final site preparation documents, two complete sets of CAD drawings, and detailed installation instructions.

3.1.3.2. The installation instructions shall clearly specify the point at which the Contractor assumes responsibility for utility connections. It is the Government's responsibility to follow the drawings provided and instructions to ensure proper site preparation for installation. In preparing the drawings, the Contractor shall make maximum use of existing infrastructure, including wall and ceiling mounts, junction boxes, raceways, and conduits. All power line recommendations must conform to the NFPA 70, National Electrical Code (NEC) (2026) Edition, or any subsequent updated version.

3.1.3.3. The Contractor shall designate a responsible and knowledgeable representative to explain the documents required in Paragraph 3.1 and implement any necessary revisions. Upon request by the Government, this representative shall visit the installation site to review and clarify the documents. Multiple site visits may be required if significant changes are necessary.

3.1.3.4. Any changes required to complete the installation due to incomplete or erroneous drawings and/or instructions provided shall be the responsibility of the Contractor.

3.1.4. Power Conditioning:

3.1.4.1. For installation and extended installation, when preparing an offer for a prospective delivery order, offerors shall assess the adequacy of the existing electrical power system for operating the proposed DIN-PACS system, which may require a visit to each installation at no cost to the Government. The Contractor shall provide appropriate protective methodologies or devices to safeguard the entire system against:

(a) Damage resulting from electrical power issues, including brownouts, emergency power interruptions, electrical surges, sags, electrical storms, and similar disturbances; and

(b) Image degradation caused by electrical power fluctuations.

3.1.4.2. Any components susceptible to power line transients shall be protected by power line transient suppressors, which shall be included in the system price.

3.2. Networking and Interfacing:

3.2.1. For all delivery orders, and independent of any on-site installation requirements, the Contractor shall provide networking, interfacing, and integration as required to support the installation and operation of the DIN-PACS system. Such services may involve existing equipment, new equipment, or the integration of new equipment with existing systems. All such services shall be offered on a delivery order basis. The costs associated are not included in the standard price of the DIN-PACS solution and shall be negotiated separately. The Contractor shall ensure that all proposed solutions are tailored to the unique infrastructure and operational needs of each installation, and that integration activities are fully documented and coordinated with the Government prior to implementation.

3.2.2. Hybrid Deployment: When applicable, the Contractor shall ensure that installation supports hybrid environments, enabling seamless integration between on-premises infrastructure and Government managed or controlled cloud infrastructure.

3.2.3. Networking & Interoperability: When applicable, the Contractor shall ensure that all networking and interoperability requirements are addressed during installation and extended configuration of the DIN-PACS system. This includes validation of IHE profiles such as XDS-I, IOCM, and PIX/PDQ to guarantee standards-based data exchange. Contractors must conduct integration testing with DoD PACS systems and community partners to confirm seamless interoperability across federal and external environments. In addition, the Contractor shall establish secure APIs to support interoperability with healthcare standards including HL7, FHIR, and CCOW/JLV, ensuring secure and reliable data sharing across platforms. Finally, installation must incorporate site-specific network segmentation and firewall configuration to strengthen security, optimize performance, and align with federal cybersecurity requirements. To demonstrate compliance, Contractors shall provide documentation showing adherence to relevant **NIST SP 800-53 (Rev. 5)** controls, including **SC-7 (Boundary Protection)**, **SC-32 (Information System Partitioning)**, **SC-31 (Cryptographic Module Authentication)**, **SI-4 (System Monitoring)**, and **AU-2 (Audit Events)**. These controls collectively ensure secure network segmentation, validated interoperability, continuous monitoring, and accountability across all networked components, thereby supporting FISMA compliance and safeguarding sensitive medical imaging data.

3.2.4. AI & Workflow Enablement: When applicable, the Contractor shall ensure that installation activities include the deployment, activation, and configuration of Augmented Intelligence (AI) modules and associated workflow engines. The Contractor shall validate that these modules are properly integrated into the clinical environment, confirm that automated processes function as intended within established workflows, and demonstrate that structured reporting templates are pre-loaded, tested, and operational. Installation shall be performed in a manner that ensures interoperability, standardized documentation, and seamless incorporation of AI-enabled processes into ongoing clinical operations. To demonstrate compliance, Contractors shall provide documentation showing adherence to relevant NIST SP 800-53 (Rev. 5) controls, including:

(a) SI-4 (System Monitoring) for continuous oversight of AI module performance and workflow automation;
(b) SI-2 (Flaw Remediation) to ensure timely updates and corrections to AI algorithms;
(c) AU-2 (Audit Events) and AU-6 (Audit Review, Analysis, and Reporting) to track AI-driven workflow decisions and peer review activities.
(d) SC-28 (Protection of Information at Rest) and SC-31 (Cryptographic Module Authentication) to safeguard structured reporting data and ensure secure AI module deployment.
(e) CM-6 (Configuration Settings) to enforce standardized installation and validation of workflow engines.

These controls collectively ensure that AI-enabled functionality and workflow automation are secure, auditable, and compliant with federal standards.

Additionally, Contractors shall confirm that structured reporting and workflow validation align with FDA guidance on medical device software and ONC interoperability standards (HL7, FHIR, DICOM SR), ensuring that AI-enabled imaging workflows are both clinically safe and interoperable across VA, DoD, and community partner systems.

3.2.5. Clinical Environment Readiness: The Contractor shall ensure that all aspects of clinical environment readiness are addressed during installation and validation of the DIN-PACS system. This includes the deployment and validation of dose monitoring systems to support patient safety and compliance with radiation exposure standards, aligned with SI-4 (System Monitoring) and SI-2 (Flaw Remediation) to ensure continuous oversight and timely updates.

3.2.6. Extended Installation Enhancements: The contractor shall ensure that extended installation activities address advanced infrastructure and resiliency requirements for the DIN-PACS system. When applicable, this includes expanding HVAC and shielding specifications to support AI server clusters and GPU racks, aligned with PE-14 (Environmental Controls) and PE-15 (Water Damage Protection) to maintain environmental stability and safeguard equipment. Installation must also incorporate power conditioning beyond transient suppressors, with UPS systems sized for PACS/VNA workloads, consistent with PE-9 (Power Equipment and Cabling) and CP-7 (Alternate Processing Site) to ensure uninterrupted operations.

SOW Appendix 4 – Inspection and Acceptance

4.1 System Acceptance Inspection Testing

4.1.1. General

4.1.1.1. The Government Acceptance Testing (AT) shall include a comprehensive inspection and verification of the functional operation of the Contractor-provided system, including all ancillary components and any extended installation. The Government reserves the right to verify that the system and any extended installation comply with the requirements specified in this solicitation, resultant contract, as well as with the Contractor's published specifications and data sheets submitted with the technical proposal, and additional delivery-order level Government requirements or Contractor documentation.

NOTE: If the Contractor's specifications exceed the Government's requirements, the Government will conduct testing and base system acceptance on those higher standards. In all other cases, if a conflict arises between the Contractor's published literature and the requirements of the delivery order, including this solicitation, the requirements of the delivery order shall take precedence. Any redesign or modification of the Contractor's standard product made to meet delivery order requirements will be carefully evaluated for adequacy and suitability. Failure to comply with any specified requirement or the presence of one or more defects may constitute grounds for system AT non-compliance.

4.1.1.2. The Contractor is responsible for ensuring and demonstrating, in the presence of the Government inspection team, that the Contractor-provided system—including all hardware, software, firmware, and any extended installation—complies with the requirements of the delivery order. The Government reserves the right to conduct any inspections or tests deemed necessary to verify that all supplies, services, and equipment conform to the prescribed requirements. The Government shall have unrestricted access to the site during all phases of the project to observe every aspect of construction and installation. The Contractor is also responsible for assembling and providing all necessary equipment and personnel required to demonstrate, explain, and test the full functionality and capabilities of the Contractor-provided system and any extended installation.

4.1.2. Notice of Readiness to Inspect (NRTI)

The following NRTI procedures apply to delivery orders that require AT, as specified in the delivery order.

4.1.2.1. Upon completion of installation of all equipment and system software comprising the system (and any extended installation) as defined in the delivery order, the Contractor shall furnish a written Notice of Readiness to Inspect (NRTI) for the system.

4.1.2.2. If multiple installation sites are included in the delivery order, the Contractor shall send a separate email notification for each site.

4.1.2.3. All notifications shall be sent as follows:

For DLA Delivery Orders: email to PACSNRTI@dla.mil. On the notification email, the Contractor shall carbon copy the Authorized Customer Point of Contact (POC), Technical POC(s), Contracting Officer, and Government Acceptance Testing POC noted in the delivery order, along with any others required to be notified as per the instructions in the delivery order.

For VA Delivery Orders: email the Authorized Customer POC, Technical POC(s), Government Acceptance Testing POC, VA Contracting Officer (CO), and the Biomedical Engineer.

4.1.2.4. The date the Government receives the NRTI will be referred to as the "NRTI Date" throughout this Appendix.

4.1.2.5. The subject line of the email shall begin with "NRTI – " followed by the site name and delivery order number. For DLA Orders the subject line shall also include the applicable CLINs to be inspected.

4.1.2.6. The body of the email shall include the following:

(a) Contractor's basic contract number and delivery order number;
(b) CLINs to be inspected, along with descriptions;
(c) Installation location (hospital/facility name, room number, base/city/state);
(d) Contractor's Notification POC: name, title, telephone number, and email address;
(e) Contractor's Inspection POC: name, title, telephone number, and email address; and
(f) Certification of the following:

(1) The system is installed;
(2) The system is ready for acceptance testing;
(3) The system complies with the manufacturer's specifications and all requirements of the Government specifications defined herein; and
(4) The system meets the requirements outlined in the delivery order.

Any exceptions to the above certifications must be agreed upon by the Authorized Customer POC and pre-approved by the Contracting Officer prior to the Contractor submitting the NRTI.

4.1.2.7. The Contractor shall also submit data (completed charts or screen capture images) verifying that all diagnostic and clinical monitors, if included in the delivery order, have been properly calibrated to the required

specifications. The Contractor must also include a detailed component and master parts list for the system, as specified in Appendix 2, CDRL AC.

4.1.2.8. An automated WAWF receiving report submission notification does not satisfy the NRTI requirement.

4.1.2.9. The Contractor shall make a best effort to provide an estimated date of NRTI submission to the Authorized Customer POC approximately 2–3 weeks in advance. While this estimate is not binding, it will help both the Government and Contractor plan personnel schedules more effectively.

4.1.3. Start of Acceptance Inspection Testing

4.1.3.1. Government costs for the initial AT of supplies and services provided in accordance with the requirements specified herein shall be borne by the Government. The Contractor shall not be reimbursed for any Contractor costs incurred as a result of conducting AT.

4.1.3.2. The date on which AT begins will be referred to as the "AT Start Date" throughout this Appendix. The date on which AT is completed will be referred to as the "AT Completion Date" throughout this Appendix.

4.1.3.3. The Authorized Customer POC and the Contractor are authorized to establish the AT Start Date without intervention from the Contracting Officer. The Contractor shall "reply all" to the initial NRTI email to communicate the mutually agreed upon AT Start Date at least three business days prior to the scheduled AT. Any disagreements that arise must be coordinated through the Contracting Officer.

4.1.3.4. The Government shall have 45 calendar days from the NRTI Date to initiate AT. If a mutually agreed upon AT Start Date is not established within 30 calendar days after the NRTI Date, the Contractor must immediately notify the Contracting Officer and the Authorized Customer POC via email.

4.1.4. Performance Standard for Documentation: The Contractor shall certify that the manufacturer's manuals provided with any equipment and any software accurately reflect the configuration of the delivered equipment and software, as well as their operation and maintenance.

4.1.5. AT Procedure

4.1.5.1. AT shall be conducted only on a completely installed system, including any required integration(s). The AT consists of a series of validation steps for each requirement specified in the delivery order and DIN-PACS contract and may include tests to verify both individual component performance and overall system performance.

4.1.5.2. Testing shall be performed in accordance with the Government's AT Protocol (or another protocol if mutually agreed upon by both the Authorized Customer POC and the Contractor), using the most current version available at the time of testing. Soft copies of the AT Protocol may be obtained from the applicable site's DIN-PACS Office.

4.1.5.3. The Contractor shall be responsible for connecting all test equipment and operating the system during the AT. Deficiencies that are corrected during the inspection shall not constitute grounds for rejection.

4.1.5.4. Any system changes resulting from modifications to the delivery order issued prior to system go-live, which are necessary for the Contractor to meet the delivery order requirements, shall be incorporated into the inspection.

4.1.5.5. Use of the equipment during the period between completion of installation and at inspection, or between inspection and re-inspection, shall not negate the government's right to fail the system. Additionally, such use shall not determine the system warranty start date, which will be established according to the procedures outlined in Section 4.2 below.

4.1.6 Personnel Conducting AT

4.1.6.1. Government Personnel: The Government may use the following professionals (Military, Civilian, or Contractors):

(a) Contracting Officer / Contract Specialist(s)
(b) Radiologist(s)
(c) Medical Physicist(s)
(d) Computer / Network Specialist(s)
(e) Biomedical Engineer(s)
(f) Radiology Technologist(s)
(g) Logistician(s)
(h) DIN-PACS System Administrator(s)

4.1.6.2. Contractor Personnel: The Contractor shall provide qualified staff to demonstrate system features and capabilities, answer questions, and clarify any deficiencies relative to Government requirements during AT.

4.1.7. AT Report

4.1.7.1. The Government AT POC will document the results of the AT on a written Government AT Report. This individual will email the AT Report to:

For DLA Delivery Orders: PACSNRTI@dla.mil, the Authorized Customer POC, the Technical POC(s), the Contractor, and the Contracting Officer.

For VA Delivery Orders: The report will be emailed to the Authorized Customer POC, Technical POC(s), VA Contracting Officer (CO), and the Biomedical Engineer.

4.1.7.2. The date the AT Report is emailed under paragraph 4.1.7.1 will be referred to as the "AT Report Date" throughout this Appendix.

4.1.7.3. The Government AT Report, including a complete list of deficiencies found during testing, shall be provided to the Contractor within 30 calendar days of the AT Completion Date.

4.1.7.4. The Contractor must confirm any non-concurrence with the AT results, as documented in the AT Report, within 10 business days of the AT Report Date. The Contractor shall email PACSNRTI@dla.mil, the Government Acceptance Testing POC, the Authorized Customer POC, and the Technical POC(s).

4.1.8. AT Results. The AT Report will provide one of three possible results for the installed system, including any hardware, firmware, software, network integration, and extended installation:

(a) Pass without Conditions: No deficiencies noted on the AT Report;
(b) Pass with Conditions: The Contractor will be advised as to minor deficiencies; corrective action/open items will be listed. The Contractor shall correct the minor deficiencies; or
(c) Fail: The Contractor will be advised as to the deficiencies noted that caused a Fail; the Contractor shall correct all deficiencies.

4.1.9. Contractor Notifications and Responses following AT Report: The Contractor shall notify the Government of their proposed corrective action(s) to any deficiencies (*Pass with Conditions* or *Fail*) within 10 business days of the AT Report Date by emailing:

For DLA Delivery Orders: PACSNRTI@dla.mil, the Government Acceptance Testing POC, the Authorized Customer POC, the Technical POC(s), and the Contracting Officer.

For VA Delivery Orders: Email the VA Contracting Officer, the Government Acceptance Testing POC, the Authorized Customer POC, and the Technical POC(s).

The Contractor need not notify the Government of the proposed corrective action(s) if the AT Results were *Pass with Conditions* and the notice referenced in Section 4.1.10. is submitted within 10 business days of the AT Report Date.

4.1.10. When the AT result is *Pass with Conditions*

4.1.10.1. The Contractor shall email the parties listed in 4.1.9 when all minor deficiencies are corrected. This notice should be titled "Notice of Deficiency Correction" and shall include the Contractor resolution to any required corrective action/open items noted in the AT Report. The date the Notice of Deficiency Correction is received by the Contracting Office will be referred to as the "Notice of Deficiency Correction Date" throughout this Appendix.

4.1.10.2. Systems that *Pass with Conditions* do not require a formal re-inspection. The Government will inspect the Contractor's corrections to the minor deficiencies cited in the AT Report and provide the results to the Contractor, which will indicate the System acceptance or the need for further corrections.

4.1.11. When the AT Result is *Fail*

4.1.11.1. If the AT Result is *Fail*, the Government shall conduct a re-inspection with all costs incurred shall be chargeable to the Contractor.

4.1.11.2. When all corrections have been completed and the system is ready for re-inspection, the Contractor shall follow the same NRTI procedures noted in Section 4.1.2 above. The subject line of the NRTI must start with "Re-inspection."

4.1.11.3. The Contractor and Government shall follow the same AT guidelines (as noted in Section 4.1) for a re-inspection.

AT Process Overview Table:

"day" means "calendar day" unless otherwise noted.

Paragraph	Contractor Action	Government Action	Timeline
4.1.2.8	Emails estimated date of NTRI submission	-	Approx. 2-3 weeks in advance of Completion of Installation
4.1.2.1	Emails NTRI, which establishes NTRI Date	-	Upon Completion of Installation

4.1.3.3	-	Establishes AT Start Date with Contractor	Within 30 days of NTRI Date
4.1.3.3	Acknowledges AT Start Date via email	-	At least 3 business days prior to AT Start Date
4.1.3.4.	Sends alert if AT Start Date not established	-	30 days after NTRI Date
4.1.3.4.	-	Initiates AT	Within 45 days of NTRI Date
4.1.7.3	-	Emails AT Report	Within 30 days of AT Completion Date
4.1.7.4	Emails any non-concurrence with AT Report	-	Within 10 business days of AT Report Date
If AT Report indicates PASS with Conditions			
4.1.9	Emails proposed corrective actions	-	Within 10 business days of AT Report Date
4.1.10.1	Corrects Deficiencies	-	Completion of corrections affects Acceptance/ Warranty Start Dates
4.1.10.2	-	Confirms deficiencies have been corrected	
IF AT Report indicates FAIL			
4.1.9	Emails proposed corrective actions	-	Within 10 business days of AT Report Date
4.1.11.2	Emails estimated date of NTRI submission	-	Approx. 2-3 weeks in advance of Completion of Corrections
4.1.11.2	Emails NTRI, which established new NTRI Date	-	Upon Completion of Corrections
4.1.11.3	Follows same procedure as initial AT	Follows same procedure as initial AT	Same timeframes as initial inspection, using re-inspection NTRI and AT dates
Repeat procedures according to subsequent AT Report results			

4.2. System Acceptance / Warranty Start Date

4.2.1. Conditions of Acceptance

4.2.1.1. Final acceptance of supplies and services provided in accordance with the requirements specified herein will be made by the Contracting Officer based on satisfactory completion of the following:

(a) Successful completion of AT, when applicable, as specified above;
(b) Successful completion of any extended installation work; and

For DLA Delivery Orders:
(c) Delivery of all Contract Data Requirements Lists (CDRL's) purchased for a specific site.

For VA Delivery Orders:
(c) Delivery of equipment and/or deliverables.

4.2.1.2. The Final Acceptance Date and the Warranty Start Date shall both be established by the Contracting Officer using the guidelines in Section 4.2.2 below. The Contracting Officer shall provide written notification of these two dates to the Contractor and the Authorized Customer POC.

4.2.2. Scenarios

4.2.2.1. *Pass without Conditions*: The Final Acceptance Date will be the AT Report Date, and the Warranty Start Date shall be backdated to the NRTI Date.

4.2.2.2. *Pass with Conditions*:

(a) If all minor deficiencies noted in the AT Report are corrected within 30 calendar days after the AT Report Date, the Final Acceptance Date shall be the date the Government communicates confirmation that deficiencies have been corrected pursuant to Paragraph 4.1.10.2. The Warranty Start Date for the system shall be backdated to the AT Report Date.

(b) If the Contractor fails to correct all minor deficiencies noted in the AT Report within 30 calendar days after the AT Report Date, the Final Acceptance Date shall be the date the Government communicates confirmation that deficiencies have been correct pursuant to Paragraph 4.1.10.2. The Warranty Start Date for the System will not be backdated and shall be the date the Government communicates confirmation that deficiencies have been corrected.

4.2.3. Default Acceptance

4.2.3.1. The Contractor is entitled to Default Acceptance under the following scenarios:

(a) If the AT has not commenced within 45 calendar days from the NRTI Date, the Final Acceptance Date of the system shall be established as 45 calendar days from the NRTI Date. Note that this does not waive the Government's rights to test the system. The Warranty Start Date shall be backdated to the NRTI Date.

(b) If the Government fails to provide the AT Report to the Contractor within 30 days of the AT Completion Date, the Final Acceptance Date of the system shall be established as 30 days from the AT Completion Date. Note that this does not waive the Government's rights to provide such a report at a later date and have all deficiencies corrected under the system warranty. The Warranty Start Date shall be backdated to the NRTI Date.

(c) If the Contracting Officer does not notify the Contractor of the Final Acceptance Date/Warranty Start Date within 30 calendar days from a Notice of Deficiency Correction Date, the Final Acceptance Date shall be 30 days from the Notice of Deficiency Correction Date. If the Notice of Deficiency Correction Date is:

(1) within 30 days from the AT Report Date, the Warranty Start Date shall be backdated to the AT Report Date.

(2) more than 30 days from the AT Report Date, the Warranty Start Date shall be backdated to the date the Notice of Deficiency Correction was received.

4.2.3.2. If the Contractor is entitled to Default Acceptance under any of the scenarios mentioned above, the Contractor must notify the Government of Contractor's intension to seek Default Acceptance by emailing:

For DLA Delivery Orders: PACSNRTI@dla.mil, the Government Acceptance Testing POC, the Authorized Customer POC, and the Technical POC(s). The subject line in the email should include "Notice of Default Acceptance," the site name, delivery order number, and applicable CLINs.;

For VA Delivery Orders: the VA Contracting Officer, the Government Acceptance Testing POC, the Authorized Customer POC, and the Technical POC(s).The subject line in the email should include "Notice of Default Acceptance," the site name, and delivery order number.

4.2.3.3. The Contracting Officer and Contractor may mutually agree, in writing, to extend the timeframes noted above on a delivery order basis.

4.3. AT of Other Equipment: Other systems or equipment items purchased from this contract, and not covered under the Government's DIN-PACS AT Protocol (e.g. Film Digitizers) may be tested by the Government per Section 4.1 above. Systems will be tested per manufacturer's commercial testing protocols unless an appropriate Government testing protocol is available.

4.4. Standard of Performance for Added or Replaced Components of Equipment

4.4.1. Added Components: System components (hardware, firmware, software) which are added to a system after the system has been accepted shall be subject to the AT procedures defined herein and shall be assigned a new Final Acceptance Date and Warranty Start Date.

4.4.2. Replaced Components: Replacement components (hardware, firmware, software) shall not receive a full warranty but shall have the remaining portion of the replaced devices' warranty period.

SOW Appendix 5 – Training, System Reliability, and Maintenance

All Contractors are required to offer the 12-month Warranty as described in this Appendix. Contractors that offer a Fully Integrated System (defined below) are further required to offer the Government the option of full-time on-site system administrator during the first 12 months. Additionally, all Contractors are required to offer the Government one-year Post-Warranty Maintenance option periods, with coverage-type depending on whether fully integrated systems are involved.

Products Offered	Initial 12-months	Minimum Post-Warranty Options
Fully Integrated Systems	Warranty plus optional Full-Time On-site	Options A1, A2, and B
Modular or Deconstructed Systems	Warranty	Options A2 and B

All Contractors are additionally required to satisfy the Training requirements in Section 5.9

5.1 Definitions

(a) Component: A Component is any Contractor-provided hardware, firmware, and software including: databases, servers, storage/archive devices, workstations (diagnostic, review, quality control (QC)), hard copy devices, network peripherals, switches, teleradiology servers, imaging software, and interfaces to Government-furnished systems.

(b) Component Failure: A Component Failure is a malfunction of a Component or any part thereof that prevents the Component from performing its function and requires corrective action. Subcomponent failure (e.g., monitor) constitutes component failure (e.g., workstation).

(c) Emergency Maintenance: unscheduled immediate corrective actions required to restore clinical operation following a Component Failure.

(d) Fully Integrated System: a system containing databases, servers (including Web), intermediate and long-term storage, network switches, and all other Components necessary to have a clinically operational system.

(e) Modular or Deconstructed System: a system composed of multiple interoperable components that may be sourced from one or more contractors, in which each component performs a distinct system function.

(f) Standard Service Hours: Standard Service Hours are 0800 to 1700 local time of the site(s), Monday through Friday, excluding Federal Holidays. Some variation may occur pursuant to paragraph 5.2.8.

(g) Update: Hardware, software, or firmware changes that are backward compatible and update, fix, or improve existing functionality of a system.

(h) Upgrade: A major change that is not backward compatible and involves changes that provide additional features and functionality to an existing system. Upgrades typically involve replacing or adding new components, features, or versions of software or hardware to provide a substantial improvement in performance, functionality, or capabilities.

5.2. Warranty

5.2.1. The Contractor shall provide a twelve-month warranty, beginning on the Warranty Start Date established in Appendix 4. During this warranty period, the Contractor shall provide on-site and remote support, including preventive and corrective actions, for the System and all associated hardware, firmware, and software including upgrades - if required to remedy any incompatibility or interoperability issues that can only be resolved through replacement of the software or the current software version.

Furthermore, the Contractor shall furnish all tools, test equipment, diagnostic devices, parts, supplies, labor, travel, and any other resources necessary to meet their warranty obligations. All such support shall be provided at no additional cost to the Government, except when maintenance or repair is required due to Government abuse, misuse, misconduct, or other gross or willful damage.

The System shall meet the reliability standards specified in Paragraph 5.5.

5.2.2. Software Updates are intended to maintain the continued security, stability, and proper operation of the PACS throughout the supported lifecycle of the software (including third-party software). Accordingly, the Contractor shall provide, at no additional cost to the Government, all Updates necessary to address essential operational and security needs. These Updates shall include, but are not limited to, security patches, vulnerability remediation, bug fixes, error corrections, performance improvements, and compatibility updates required to ensure ongoing interoperability with operating systems, modalities, network environments, and applicable data and cybersecurity standards.

Updates shall be provided for the full duration of the software’s published service life. The Contractor shall not require the Government to purchase Upgrades or replacement software to maintain interoperability, compatibility, or secure operation when the currently deployed version has not reached its end-of-service life. If an Upgrade is the only viable means to correct an incompatibility, interoperability issue, or security vulnerability, the Contractor shall provide that Upgrade at no additional cost to the Government.

If any Update or Upgrade adversely affects system interoperability, performance, or functionality, the Contractor shall, at no additional cost, provide all corrective actions necessary to restore proper and reliable operation. All

Updates and associated corrective actions shall be delivered in a manner that maintains stable system performance and shall not introduce new features beyond those required to preserve secure and proper functionality.

Timelines regarding vulnerability management shall be addressed at the delivery order level.

5.2.3. The Contractor shall perform all maintenance in an expedient manner that minimizes system downtime and promptly restores clinical operations and patient care. All services shall be performed by factory-trained, English-speaking, technically qualified, and authorized personnel.

5.2.4. The Contractor shall maintain an available point of contact, accessible 24 hours a day, 7 days a week, to ensure issues, incidents, or service interruptions can be reported and addressed without delay, and shall copy the Contracting Officer and the Technical POC listed in the delivery order on all responses.

5.2.5. Acknowledgment: The Contractor shall acknowledge a formal notification of the need for Emergency Maintenance within one hour of receipt, regardless of when the notification is made, and copy the contracting officer and technical POC listed on the delivery order. The Contractor shall acknowledge a formal notification of the need for non-Emergency Maintenance within four hours of receipt, regardless of when the notification is made. Acknowledgements outside the Standard Service Hours shall occur at no additional cost to the Government.

5.2.6. Corrective Action:

5.2.6.1 Emergency Maintenance: If the Contractor receives formal notification within the Standard Service Hours that Emergency Maintenance is required, the Contractor shall start corrective action, either remotely or on-site, within four hours of receiving the formal notification, even if the service starts outside the Standard Service Hours. Once corrective action has begun, it shall continue during Standard Service Hours until all repairs are completed, all integrated performance parameters are being met, and the system is available for clinical use. Emergency Maintenance is covered under Warranty at no additional cost to the Government, including work performed outside the Standard Service Hours when required above.

5.2.6.2. Unscheduled Corrective Maintenance: Corrective action to repair Component Failures that are not affecting clinical use of the system shall be performed within 24 hours of receipt of the Government's formal notification of the need for corrective action. Any work shall be performed only during Standard Service Hours unless otherwise coordinated with the site. Any work so coordinated is at no additional cost to the Government.

5.2.7. Preventative maintenance shall only be performed as scheduled. The Contractor shall coordinate preventative maintenance with the Government's site(s) representative(s) and obtain approval of the schedule. Service reports of all scheduled services shall be maintained and provided to the Government POC for verification, and to the Contracting Officer upon request. The Contractor shall also maintain historical service records for each Component, which shall be made available to the Government upon request. To the maximum extent possible, preventative maintenance shall be performed on individual Components to avoid impacting the operation of the entire System. If preventative maintenance adversely affects System operation, the Contractor shall coordinate the maintenance with site.

5.2.8. On a delivery order basis, Contractors will be required to provide offers for Standard Service Hours and Response times that vary from the Government's standard. Contractors are encouraged to include in their proposals alternate pricing for expanded service hours (e.g. second shift, weekends, federal holidays, etc.) and alternate standard response times.

5.2.9. Remote Diagnostics and Tele-maintenance.

5.2.9.1. Utilization of DoD DISA or VA approved B2B Gateway (as applicable), for DIN-PACS Support: The Contractor shall demonstrate and provide system connectivity, diagnostic software, and technical support services that use the DoD DISA Business to Business (B2B) gateway for troubleshooting, repairing, and configuring DIN-PACS products.

5.2.9.2. B2B Gateway Requirement: The Business to Business (B2B) gateway shall be able to reach all central system Components in the DIN-PACS (i.e. servers, database, archive controller, archive devices, routers, and network management workstations) through a common (single) telecommunications access line.

5.2.9.3. Tele-Maintenance and Advanced Remote Support Capabilities: Contractors shall use tele-maintenance methods that include telephonic communication with Government site support staff and users, as well as modern remote technologies such as secure video conferencing for real-time troubleshooting and training. The Contractor is encouraged to provide additional diagnostic and support capabilities, when available or applicable, including Internet-of-Things-enabled monitoring for continuous system oversight, Augmented Intelligence-driven predictive analytics to anticipate and mitigate potential failures, mobile applications to facilitate field technician access and collaboration, augmented reality (AR) support tools to deliver guided repair and configuration assistance, and collaboration platforms to ensure effective documentation, workflow management, and technical support. The Contractor shall provide training programs for staff and end users and describe the tele maintenance support program for remote diagnostics and assistance.

5.2.9.4. Online Help Desk: Contractors shall provide sites with online access to a computer-based help desk. The Online Help Desk shall allow customers to request scheduled and unscheduled services, query historical data, and generate reports. The Online Help Desk shall provide real time information, including current status, total equipment downtime, service ticket initiator, original complaint, response time, assigned technician, work performed, replacement parts, and completion date and time.

5.2.10. Service Report Documentation

5.2.10.1. Documentation and Submission Requirements: All service reports - scheduled and corrective - shall be documented, validated by the Government POC, and provided to the appropriate on-site Government representative. The Contractor shall also provide service reports to the Contracting Officer upon request. Reports shall be filed with the equipment history file and submitted in accordance with applicable Military Service policies and procedures.

5.2.10.2. Minimum Report Content: At a minimum, each report shall include the following information listed in the table below:

Minimum Required Report Entries	
(a)	Date and time of notification
(b)	Date and time of arrival on-site
(c)	Description of malfunction or service performed
(d)	Model number, serial number, and equipment location
(e)	Time spent on repair
(f)	Parts used or replaced
(g)	Parts cost
(h)	Description of service performed
(i)	Name of Government POC
(j)	Name of Contractor service engineer
(k)	Tele-maintenance methods used, if applicable
(l)	Designation of user error, if applicable

5.3. Full-Time System Administrator Option

In addition to the requirements under 5.2, for Fully Integrated Systems, the Contractor shall offer the government a fulltime on-site administrator satisfying the following requirements.

5.3.1. Contractor Responsibilities.

5.3.1.1. The level of service support required shall be determined by the size and complexity of the system.

5.3.1.2. The Contractor shall provide the Government with the option of fulltime, on-site Contractor System Administrator(s) dedicated to system maintenance, training, and administration. The Contractor shall ensure that such personnel possess the necessary qualifications, experience, and authority to perform all required functions effectively, and shall make this option available independent of any other service agreements. The Contractor shall provide personnel qualifications upon request.

5.3.1.3. The Contractor shall provide or make available full-time on-site technical support at the time of initial clinical use and shall ensure that such support remains continuously onsite throughout the warranty period, including any extensions thereof. The Contractor guarantees that the Contractor's System Administrator(s) is present and available to perform system maintenance, training, and administration functions as required, without interruption, for the duration of the applicable warranty coverage.

5.3.1.4. Maintenance plans must clearly define the number and qualifications of on-site maintenance staff, scheduled calibration, electrical safety testing, and preventive maintenance programs, repair procedures and escalation protocols, archive system maintenance requirements, and database maintenance plans including updates, optimization, and integrity checks. These plans shall also specify the repair parts program, including availability and replacement timelines, technical support resources, and facilities requirements necessary to perform maintenance activities (including training, travel, and tele-maintenance).

5.3.1.5. Shift Coverage and On-Call Support Obligations: Full-time technical support shall be provided by the Contractor and shall be physically present on-site during the first shift. For the second and third shifts, the Contractor shall ensure that qualified technical support personnel are available on an on-call basis. The response and resolution requirements for the second and third shifts are defined as follows:

Initial Response: The Contractor shall acknowledge and begin remote triage of any reported issue within 30 minutes of notification.

Remote Resolution: The Contractor shall provide active remote troubleshooting and aim for corrective action within 1 hour of the initial response, consistent with Appendix 5 requirements for maintaining system functionality.

On Site Dispatch (if required): If an issue materially affects clinical operations and cannot be resolved remotely, the Contractor shall begin on-site corrective action within 4 hours of the initial formal notification.

These response expectations apply to all system issues reported during second and third shifts and shall be aligned with the severity based maintenance requirements in Appendix 5. The Contractor shall guarantee uninterrupted coverage across all shifts and shall ensure that personnel assigned to these obligations possess the qualifications necessary to maintain continuous system functionality.

5.3.2. Government Responsibilities.

5.3.2.1. System Engineering: Government facility support personnel shall ensure the optimal operation of all computer components of the DIN-PACS system. Responsibilities include managing and overseeing databases, image transmission processes, and network operations across both local area networks (LAN) and wide area networks (WAN). Personnel shall also maintain and support interfaces to imaging modalities, image display systems, and electronic image archives to ensure continuous, reliable, and secure system performance in accordance with contractual and operational requirements.

Note: When these systems are under warranty or covered under maintenance Option A1, the contractor shall perform these functions.

5.3.2.2. Archive/Database Management (Government Systems): Government facility support personnel shall perform all electronic image acquisition, storage, and archiving within Government-owned systems (e.g., ECIA,

VistA Imaging, CareAware MultiMedia (CAMM)). When these systems are under warranty or covered under maintenance Option A1, the contractor shall assume these responsibilities.

In all other cases, personnel shall ensure that images are stored in the correct format, accurately linked to exam data, and readily accessible for physician review and diagnosis. Personnel shall demonstrate proficiency in computer-based data management and in the operation and troubleshooting of Government-managed image archive systems.

Additionally, all contractor-managed systems—including enterprise EHR systems and VNA systems—shall be fully maintained by the contractor.

5.3.2.3. Computer Technical Skills/Training: The Government's facility support personnel shall be responsible for basic system maintenance and training in system operation. Personnel shall demonstrate competence in all aspects of computer system maintenance and possess a thorough understanding of electronic circuits and troubleshooting techniques. Personnel shall demonstrate proficiency in preventive maintenance, calibration, and safety testing of image display workstations and related equipment is required. Personnel shall be proficient in operating all system components and fully capable of training others in proper equipment use.

5.4. Post-Warranty Maintenance

5.4.1. The Contractor shall provide a post-warranty maintenance program for each installed system, covering up to five option years following the conclusion of the one-year warranty period.

5.4.2. There are three possible scopes of work for the post-warranty maintenance program, to be determined at the delivery-order level:

5.4.2.1 Option A1 (Basic plus on-site)

(a) Services and system reliability requirements shall be the same as those of the warranty period in Section 5.2.
(b) On-site services shall be the same as those in Section 5.3.

5.4.2.2. Option A2 (Basic)

(a) Services and system reliability requirements shall be the same as those of the warranty period in Section 5.2.
(b) Section 5.3 does not apply.

5.4.2.3. Option B (Shared)

(a) Services and system reliability requirements shall be the same as those of the warranty period in Section 5.2, except as modified by paragraph (c) below.
(b) Section 5.3 does not apply.
(c) Shared maintenance is performed by the Government with the following provisions:

(1) Government Responsibilities:

(A) The Government shall perform the first call on all service requests.
(B) The Government shall perform additional services under tele-maintenance guidance.
(C) The Government shall conduct scheduled maintenance for components identified in a mutually agreed maintenance allocation chart.
(D) The Government shall purchase supplies required for scheduled services it performs.

(2) Contractor Responsibilities

(A) The Contractor shall develop a maintenance allocation chart detailing Government and Contractor responsibilities; final allocations shall be site-specific and mutually agreed.
(B) The Contractor shall provide factory-level training for all services performed by the Government.
(C) The Contractor shall perform all remaining scheduled services and repairs, including parts, labor, and travel.
(D) The Contractor shall provide on-site support for system operation and maintenance only.
(E) The Contractor shall provide software Updates to installed system functionality at no additional cost to the Government.

5.4.3. Commercial Post-Warranty Maintenance Plans

Contractors are encouraged to offer their normal commercial maintenance service plans, based on their standard commercial maintenance service terms and conditions, in addition to the Government-specified service options described above. If such commercial plans are offered, the Contractor shall provide the following:

(a) Acknowledgement that while contractors can propose their usual commercial maintenance plans, these are supplemental to the Government's required options.

(b) The methodology or process used by the Contractor to calculate the maintenance service price for a specific medical treatment facility (e.g., price calculated as a fixed percentage of equipment cost).

(c) A comparison of the Contractor's standard commercial maintenance service terms and conditions with the Government's scope of work Options specified in Section 5.4.2 above.

(d) Firm, fixed price post warranty maintenance proposals for five option years, to be submitted prior to award of each site-specific delivery order. Pricing shall normally be required for each of the Government-specified service options, as well as for any vendor commercial plan offerings.

5.5. Reliability Requirements

5.5.1. The system shall maintain a minimum of 99.9% Uptime during the initial warranty period. This same uptime requirement of 99.9% continues into the Post-Warranty period, ensuring long-term reliability. In addition to system-level targets, all Components must achieve a minimum quarterly 99.9% uptime, preventing weak links and ensuring consistent performance across subsystems. Downtime starts upon Government notification of the component failure to the designated Contractor POC and ends when repairs are complete, all performance parameters are being met, and the component/system is clinically operational. Downtime shall not include mutually approved scheduled maintenance and installation or modification of software, firmware, or hardware (e.g. updates/upgrades); and system failures due to operator abuse, natural disasters, or events clearly beyond the control of the Contractor.

Multiple failures to meet this requirement over a three consecutive month period may be grounds for termination for cause under paragraph (m) of clause 52.212-4, Terms and Conditions -- Commercial Products and Commercial Services (FEB 2026) RFO DEVIATION 2026-O0038.

5.5.2. Adjustments for Option B under Post Warranty Maintenance Program

The Contractor's uptime responsibility shall be modified as follows:

(a) Downtime begins only after the Government completes all first call and tele-maintenance efforts and the Contractor arrives on-site.

(b) Contractor must respond telephonically within 1 hour and arrive on-site within 12 hours of determining that on-site intervention is required.

(c) For geographically remote sites, longer response times and additional costs may be negotiated on a delivery-order specific basis.

5.6. All maintenance activities shall be conducted in accordance with applicable industry standards, manufacturer specifications, relevant laws and regulations, and contractual service level agreements to ensure compliance, safety, and reliability.

5.7. Service not covered by this Appendix, such as corrective maintenance performed outside of the Standard Service Hours (except when required for Emergency Maintenance as detailed in 5.2.3), is not covered under this contract. Such maintenance shall only be performed on a separate contract established by the site's Contracting Officer. Parts costs incurred during such maintenance calls shall be included in this contract's base warranty/maintenance price and shall not be billed separately to the customer. Any scheduling by the vendor to perform work outside hours covered under this contract to minimize system downtime impact is done at no additional cost to the government.

5.8. Compliance with Government Security and Access Requirements: Contractor maintenance personnel will be required to comply with all site-specific Government base and IT network access requirements, to include, but not be limited to, successfully completing National Agency Checks (NACs) and obtaining Common Access Cards (CACs). The Contractor shall be responsible for ensuring that all required clearances, credentials, and access authorizations are obtained and maintained for the duration of the contract.

5.9. Training

5.9.1. Site-Specific Training Requirements: Training shall be purchased on a delivery order basis to meet the unique requirements of each medical treatment facility.

5.9.2. Contractor Training Offerings: Contractors are encouraged to offer a broad range of commercial training programs for staff and system end users to ensure flexibility and comprehensive coverage of user needs, including on site and virtual training sessions for end users and administrators, supported by 24/7 technical assistance with defined response times to maintain continuous operational readiness.

5.9.3 Training Session Identification and Roster: The Contractor shall identify the number of proposed training sessions, the number of trainees that may attend each session, and the duration of each session included with the purchase of the system. Following completion of training, the Contractor shall provide the site with a training roster listing all trainees, including names, roles, and dates of participation. The roster will also be available upon request to the contracting officer.

5.9.4. Training Delivery Methods: Training shall be delivered through one or more of the following methods: on-site classroom instruction, virtual instructor-led training, webinars, or blended learning formats. The Contractor shall ensure that delivery methods are compatible with DoD cybersecurity and accessibility requirements.

5.9.5. Training Updates: The Contractor shall update training materials and sessions as system functionality evolves, ensuring that training remains current with all software updates, hardware changes, and procedural modifications.

SOW Appendix 6 – Cybersecurity

6.1. DoD Orders

For the purposes of this solicitation, Cybersecurity, Risk Management Framework (RMF), and Information Assurance (IA) requirements are used synonymously to refer to the same set of DoD Cybersecurity regulations and policies.

6.1.1 All PACS are required to meet DHA and individual Military Service Cybersecurity requirements. Cybersecurity requirements mandate that all PACS, including third-party components, receive an Authorization to Operate (ATO) or RMF Approval before being connected to any DoD network. ATO or RMF Approval is DHA or Service-specific, so reciprocity is dependent on which Services are involved and is not guaranteed. As the requirements may change, the

latest specific Cybersecurity requirements should be obtained from the DLA Contracting Officer prior to submitting an offer. Failure to agree to DHA or Service Cybersecurity requirements may result in rejection of the Contractor's offer. Failure to disclose that a system cannot meet Cybersecurity requirements, failure to meet certification timeframes, or failure to receive ATO or RMF Approval may result in a delivery order being terminated for cause in accordance with FAR 52.212-4(m).

6.1.2. The vendor shall monitor and comply with the most recent versions of the following regulations, guidance, and publications. Where conflicts exist between references, the more stringent requirement shall apply. Updates to any referenced document shall be incorporated into the vendor's process within 90 days of publication, unless otherwise directed by the Government.

(a) United States Law

(i) The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
(ii) The Federal Information Security Management Act (FISMA)
(iii) The E-Government Act of 2002
(iv) H.R.2617—Consolidated Appropriations Act, 2023, Section 524B, Ensuring Cybersecurity of Devices
(v) Section 889 of Public Law 115-232 (2019 National Defense Authorization Act (NDAA)), Parts (A) and (B)
(vi) 15 CFR Part 791, Securing the Information and Communications Technology and Services Supply Chain (December 6, 2024)

(b) Executive Orders
(i) Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 2019
(ii) Executive Order 14028, Improving the Nation's Cybersecurity, May 2021

(b) Office of Management and Budget (OMB)

(i) Circular A-130, Managing Information as a Strategic Resource
(ii) Guidance M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12-Policy for a Common Identification Standard for Federal Employees and Vendors
(iii) OMB Memorandum M-26-05 (rescinding M-23-16 and M-22-18), Adopting a Risk-Based Approach to Software and Hardware Security, January 2026

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

(i) NIST Special Publication (SP) 800-37 Rev. 2—Guide for Applying the 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 Rev. 5—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

(d) National Institute of Standards and Technology (NIST)
(i) NIST Special Publication (SP) 800-37 Rev. 2, 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 Rev. 5, 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 800-218, Secure Software Development Framework (SSDF)

(e) Federal Information Processing Standards (FIPS)

(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 201-3, Personal Identity Verification of Federal Employees and Vendors

(f) Department of War (DoW)

(i) DoW Instruction 5200.02, DoW Personnel Security Program (PSP)
(ii) DoW Instruction 8500.01, Cybersecurity
(iii) DoD Instruction 8510.01, Risk Management Framework (RMF) for DoW Information Technology
(iv) DoW Instruction 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
(v) DoW Instruction 8551.01, Ports, Protocols, and Services Management (PPSM)
(vi) DoW Instruction 8580.02, Security of Individually Identifiable Health Information in DoW Health Care Programs
(vii) DoW Instruction 6025.18, Privacy of Individually Identifiable Health Information in DoW Health Care Programs
(viii) DoW Directive 5400.11, DoD Privacy Program
(ix) DoW CIO Memorandum on Commercial Off-the-Shelf (COTS) Information and Communications Technology Supply Chain Risk Management, June 2025

(g) Cybersecurity and Infrastructure Security Agency (CISA)
(i) CISA Minimum Elements for a Software Bill of Materials (SBOM), August 2025 (Draft)
(ii) CISA Hardware Bill of Materials (HBOM) for Supply Chain Risk Management, September 2023

General contractor requirements, system security requirements, as well as access information, are located on the DoD Cyber Exchange Website: https://public.cyber.mil. Additionally, contractor guidance on Common Access Cards (CAC) and PKI can be found at: https://public.cyber.mil/pki-pke/.

6.1.3. All DIN-PACS shall support Internet Protocol version 6 (Ipv6).

6.2. VA Delivery Orders

VA Special Contract Information Technology Requirements

Minimum Statutory Requirements

At a minimum, maintenance/installation (warranty) contracts in which VA sensitive information and/or systems are accessed by a VA contractor/subcontractor require the following five requirements per 38 U.S.C. §§ 5723 and 5725:

A prohibition on unauthorized disclosure: Information made available to the contractor or subcontractor by VA for the performance or administration of this contract, or information developed by the contractor in performance or administration of the contract, shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. See VA Handbook 6500.6, Appendix C (VA Notice 24-12), paragraph 3.a., and "VA sensitive information" includes Sensitive Personal Information (SPI) as defined in VA Handbook 6500.6. Unauthorized use includes cloud storage, third-party processing, or AI tools not expressly authorized by VA.

A requirement for data breach notification: Upon discovery of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access, the contractor/subcontractor shall immediately and simultaneously notify the COR, the designated ISO, and Privacy Officer for the contract. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. See VA Handbook 6500.6, Appendix C, paragraph 6.a. Note: Notification must occur within one

hour of discovery and include reporting to the COR, CO, ISO, and Privacy Officer. The COR shall receive the report from the contractor and alert the appointed Privacy Officer.

A requirement to pay liquidated damages in the event of a data breach: "In the event of a data breach or privacy incident involving any SPI the contractor processes or maintains under this contract, the contractor shall be liable to VA for liquidated damages for a specified amount per affected individual to cover the cost of providing credit protection services to those individuals." See VA Handbook 6500.6, Appendix C, paragraph 7.a., 7.d. Also, see Section 2.5 below (LIQUIDATED DAMAGES FOR DATA BREACH).

A requirement for annual security/privacy awareness training: "Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access shall complete, on an annual basis, either: (i) the VA security/privacy awareness training (which contains VA's security/privacy requirements) within 1 week of the initiation of the contract, or (ii) security awareness training provided or arranged by the contractor that conforms to VA's security/privacy requirements as delineated in the hard copy of the VA security awareness training provided to the contractor. If the contractor provides their own training that conforms to VA's requirements, they will provide the COR or CO a yearly report (due annually on the date of the contract initiation) stating that all applicable employees involved in VA's contract have received their annual security/privacy training that meets VA's requirements and the total number of employees trained. See VA Handbook 6500.6, Appendix C, paragraph 9. Contractor-provided training must align with NIST SP 800-53 Awareness & Training controls and be pre-approved by VA. Annual reports must certify compliance with VA Handbook 6500.6 Appendix C.

A requirement to sign VA's Rules of Behavior: "Before being granted access to VA information or information systems, all contractor employees and subcontractor employees requiring such access shall sign, on an annual basis, an acknowledgment that they have read, understand, and agree to abide by VA's Contractor Rules of Behavior, which are attached to this contract." See VA Handbook 6500.6, Appendix C, paragraph 9, Appendix D. Note: Contractors must use the current version of VA's Contractor Rules of Behavior. Electronic signatures are acceptable if maintained in VA-approved systems. If a medical device contractor anticipates that the services under the contract will be performed by 10 or more individuals, the Contractor Rules of Behavior may be signed by the contractor's designated representative. The contract must reflect by signing the Rules of Behavior on behalf of the contractor that the designated representative agrees to ensure that all such individuals review and understand the Contractor Rules of Behavior when accessing VA's information and information systems.

VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY

1. GENERAL

   Contractors, contractor personnel, subcontractors, and subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

2. ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

   a. A contractor/subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

   b. All contractors, subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for contractors must be in accordance with VA Directive and Handbook 0710, Personnel Suitability and Security Program. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

   c. Contract personnel who require access to national security programs must have a valid security clearance. The National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of

Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates, the contractor/subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth.

e. The contractor or subcontractor must notify the Contracting Officer immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the contractor or subcontractor's employ. The Contracting Officer must also be notified immediately by the contractor or subcontractor prior to an unfriendly termination.

3. SANITIZATION OF SENSITIVE DATA FOR TRADE-IN EQUIPMENT

All medical equipment provided for trade-in containing electronic Protected Health Information (ePHI) will be sanitized by VA according to VA guidelines prior to release to the contractor. The media sanitization process will be as minimally destructive as possible to preserve the functioning of the equipment. Whenever possible, the operating system (OS) and application software will be preserved. If the operating system and/or application software cannot be preserved, VA will elect to use one of the following trade-in options:

i. Trade-in Option 1 – In instances where sanitization of ePHI compromises the OS and/or application software or requires the removal of internal storage media, the contractor accepts the equipment "as is" and can elect, at their discretion, to contract with the original equipment manufacturer (OEM) to restore the system.

ii. Trade-in Option 2 – In instances where sanitization of ePHI compromises the OS and/or application software, the operating system and application software will be reloaded by VA or a contractor contracted by VA on the native system drive post sanitization. Verification of system operation is the responsibility of the contractor.

4. IT CONTRACT SECURITYVA INFORMATION CUSTODIAL LANGUAGE

a. Information made available to the contractor or subcontractor by VA for the performance or administration of this contract, or information developed by the contractor/subcontractor in the performance or administration of the contract, shall be used only for those purposes and shall not be used in any other way without the prior written agreement of the VA. This clause expressly limits the contractor/subcontractor's rights to use data as described in Rights in Data – General, FAR 52.227-14(d) (1). For purposes of this clause, 'VA sensitive information' includes Sensitive Personal Information (SPI) and electronic Protected Health Information (ePHI) as defined in VA Handbook 6500.6 (2024 revision). Unauthorized use includes storage, processing, or analysis in non-VA approved environments, including cloud services or AI systems, unless expressly authorized in writing by VA.

b. VA information should not be co-mingled, if possible, with any other data on the contractor's or subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the contractor must ensure that VA information is returned to the VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on-site inspections of contractor and subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

c. Prior to termination or completion of this contract, the contractor/subcontractor must not destroy information received from VA, or gathered/created by the contractor in the course of performing this contract, without prior written approval from VA. Any data destruction performed on behalf of VA by a contractor/subcontractor must be conducted in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information

Management, and its Handbook 6300.1, Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization. Self-certification by the contractor that the data destruction requirements above have been met must be submitted to the VA Contracting Officer within 30 days of termination of the contract.

d. The contractor/subcontractor must receive, gather, store, back up, maintain, use, disclose, and dispose of VA information only in compliance with the terms of the contract and applicable Federal and VA information confidentiality and security laws, regulations, and policies. If Federal or VA information confidentiality and security laws, regulations, and policies become applicable to the VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations, and policies in this contract.

e. The contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on contractor/subcontractor electronic storage media for restoration in case any electronic equipment or data used by the contractor/subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, once the restoration is complete, the copies must be appropriately destroyed.

f. If VA determines that the contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient grounds for VA to withhold payment to the contractor or third party, or to terminate the contract for default, or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

g. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated, and appropriate actions taken in accordance with VHA Handbook 1600.01, Business Associate Agreements. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

h. The contractor/subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

i. The contractor/subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements. VA Configuration Guidelines are available upon request.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the contractor/subcontractor may use and disclose VA information only in two other situations: (i) in response to a qualifying order of a court of competent jurisdiction, or (ii) with VA's prior written approval. The contractor/subcontractor must refer all requests for, demands for production of, or inquiries about VA information and information systems to the VA contracting officer for response.

k. Notwithstanding the provision above, the contractor/subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records, and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the contractor/subcontractor receives a court order or other requests for the above-mentioned information, the contractor/subcontractor shall immediately refer such court orders or other requests to the VA contracting officer for response.

l. For services that involve the storage, generation, transmission, or exchange of VA sensitive information but do not require C&A or an MOU-ISA for system interconnection, the contractor/subcontractor must complete a Contractor Security Control Assessment (CSCA) on a yearly basis and provide it to the COR.

5. TRAINING

All contractor employees and subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:

Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Contractor Rules of Behavior, Appendix E, relating to access to VA information and information systems.

Successfully complete the VA Cyber Security Awareness and Rules of Behavior training and annually complete required security training.

Successfully complete the appropriate VA privacy training and annually complete required privacy training.

Successfully complete any additional cybersecurity or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the contracting officer for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

The contractor shall provide to the contracting officer and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 1 week of the initiation of the contract and annually thereafter, as required.

Failure to complete the mandatory annual training and sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

6. SECURITY INCIDENT INVESTIGATION

a. The term "security incident" means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets or sensitive information, or an action that breaches VA security procedures. The contractor/subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract, of any known or suspected security/privacy incidents or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the contractor/subcontractor has access.

b. To the extent known by the contractor/subcontractor, the contractor/subcontractor's notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the contractor/subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft, break-in, or other criminal activity, the contractor/subcontractor must concurrently report the incident to the appropriate law enforcement entity (or entities) of jurisdiction, including the VA OIG and Security and Law Enforcement. The contractor, its employees, its subcontractors, and their employees shall cooperate with VA and any law enforcement authority responsible for the investigation and prosecution of any possible criminal law violation(s) associated with any incident. The contractor/subcontractor shall cooperate with VA in any civil litigation to recover VA information, obtain monetary or other compensation from a third party for damages arising from any incident, or obtain injunctive relief against any third party arising from, or related to, the incident.

7. SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the contractor under the clauses contained within the

contract. With 10 working days' notice, at the request of the Government, the contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

SOW Appendix 7 – DIN-PACS Lifecycle System Support and Software Requirements

The terms Component, Update, and Upgrade shall have the same meaning as Appendix 5.

7.1. System Lifecycle Support Objectives and Contractor Commitment:

7.1.1. Main Objectives of Lifecycle Support: Contractors must provide lifecycle support to ensure that medical imaging infrastructure remains reliable, secure, and compliant throughout its operational lifespan. This includes initial deployment, integration with hospital systems, and system lifetime adherence to standards such as DICOM, FHIR, and HIPAA.

7.1.2. End of Life/End of Service Life Definitions:

7.1.2.1. End of Life (EOL): The time in a product's lifecycle where the Contractor will no longer sell or manufacture the product. During this time all support (maintenance, consumables, and accessories) will continue to be available from the Contractor for the product until it reaches its End of Service Life.

7.1.2.2. End of Service Life (EOSL) - The time in a product's lifecycle where the Contractor will no longer sell or manufacture the product and all support (maintenance, consumables, and accessories) is no longer available from the Contractor for the product.

7.1.3. Contractor Commitment: The Contractor understands and agrees to abide by the system lifecycle requirements in this solicitation. Delivery orders may have additional requirements.

7.1.3.1. If a Contractor's system reaches its EOSL or requires an Upgrade for reasons relating to Risk Management Framework (RMF) compliance prior to the expiration of the number of years specified in its offer submission for the delivery order, the Contractor shall be liable for all charges associated with such Upgrade to ensure the system remains fully operational and RMF compliant.

7.1.3.2. The sole exception to the requirement in paragraph 7.2.3.1 is when a Government-initiated adjustment to RMF requirements occurs after system installation, necessitating an Upgrade to maintain RMF compliance, including but not limited to a Government-mandated transition to an operating system different from that previously identified in the delivery order or cyber requirements.

7.2. Hardware Lifecycle Support:

7.2.1. Spare Parts Availability Guarantee: For a period of seven years following final system acceptance, the Contractor shall guarantee the Government the ability to purchase all necessary spare parts directly from the Contractor to maintain the system. Such availability shall be independent of, and not contingent upon, any post-warranty service agreements or site-specific service contracts that may be purchased by the Government. This guarantee excludes general-purpose computer hardware (e.g., PCs and servers) used within the DIN-PACS solution.

7.2.2. Hardware Support: Post-warranty support for computer hardware shall be available for a minimum of three years following the conclusion of the one-year warranty period, beginning on the date of final system acceptance, unless otherwise specified.

7.3. Software Lifecycle Requirements

7.3.1. Right to Reinstall on Replacement Hardware: The Government shall be able to reinstall vendor application software and Operating Systems (OS) on new hardware if the original hardware on which such software was installed fails, at no additional cost to the Government.

7.3.2. Software Continuity: All software provided under this contract—including the DIN PACS application software, the commercial operating system, and any third party components—shall not contain any mechanism that disables, limits, or stops software functionality due to the passage of time, release of new versions, license expiration, or any other condition not expressly identified in the original equipment purchase. The automatic extension of the Government's software subscriptions, licenses, or contracts beyond the period (or other usage parameter (e.g. volume)) covered by the purchase price is prohibited. The period may only be extended after a properly executed written agreement (or modification).

The Contractor shall ensure that all third party software complies with these requirements.

7.3.3. Software Version Requirements: Any DIN-PACS software, OS, or software that replaces an OS—including server OS, application OS, or third-party application software—must be either the latest major release currently available for commercial purchase or no more than one major release behind the latest version. Older releases may only be used if explicitly authorized in writing by the requesting Department of Defense (DoD) or other Government agency and approved by the Contracting Officer. This requirement applies broadly to all current and future architectures, including, but not limited to, Windows-hosted operating systems, IT converged infrastructure platforms, and container-based architectures.

7.3.3.1 Commercial Off-the-Shelf (COTS) Software Requirements: Furthermore, any COTS DIN-PACS software, operating system, or application software—including third-party applications such as tools for image acquisition, manipulation, reconstruction, analysis, or display—required for the operation or maintenance of any system procured under this contract must be provided by the contractor and must have a minimum service life of four years without requiring an Upgrade, as defined in Appendix 5.

7.3.3.2. Software Update Requirements: The Contractor shall provide all software updates, security patches, and minor revisions necessary to maintain operability, interoperability, and cybersecurity compliance at no additional cost to the Government. The Contractor shall also ensure that all DIN PACS components remain compatible with supported operating systems and ensure that the system remains fully supportable, secure, and compliant throughout the four year minimum sustainment period.

7.3.3.3. Four-Year System Interoperability and Supportability Guarantee: The Contractor shall guarantee that all individual software Components comprising the system (including COTS software, operating systems, database platforms, and third-party software) shall remain fully interoperable with one another and that no component shall become obsolete, unsupported, or non-sustainment eligible for a minimum period of four (4) years following Government Final Acceptance.

If, during the four-year guarantee period, an Upgrade is required to either restore interoperability between components or to prevent a component from becoming obsolete or non-compliant, the Contractor is obligated to provide and install said Upgrade at no additional cost to the Government. This obligation is in accordance with the Contractor's commitment in Section 7.1.3.1, where the Contractor is liable for all charges associated with Upgrades required for RMF compliance or to prevent a system from reaching its End-of-Service-Life (EOSL).

7.4. General Support Policies

7.4.1. Vendor Neutral Archive (VNA) Support: Contractor shall provide VNA support, including but not limited to systems such as ECIA, AGFA (IMPAX and EI), and VistA Imaging, for the duration of the system's use unless otherwise specified. This obligation ensures that the Contractor maintains continuous support for the VNA throughout its operational lifecycle, covering maintenance, troubleshooting, updates, and integration assistance as required.

7.4.2. Support Requirements Following Declined Upgrades: The Government reserves the right to decline system Upgrades, whether hardware or software. If this option is exercised, the Contractor shall continue to support the existing installed system - including hardware, software, and spare parts - for a minimum of three years following the release of the declined Upgrade. With respect to software, the Contractor shall provide support for at least the two immediately preceding versions.

7.5. Restrictions on Bundled Updates and Upgrades

7.5.1. Restrictions on Bundled Updates and Upgrades: The Contractor shall not provide an Update that is bundled with, conditioned upon, or otherwise dependent on an Upgrade (as defined in Appendix 5).

(End Statement of Work)

C03 Contractor Retention of Supply Chain Traceability Documentation (JUN 2023) DLAD

(1) By submitting a quotation or offer, the contractor is confirming it currently has, or will obtain before delivery, and shall retain supply chain traceability documentation, as described in paragraph (2) of this procurement note, demonstrating the item conforms to the technical requirements, and, for part numbered items, is from an approved manufacturer.

(2) Supply Chain Traceability Documentation

(i) Supply chain traceability documentation shall include: basic item description; part number; drawing or specification; national stock number; manufacturing source; manufacturing source's Commercial and Government Entity (CAGE) code; and clear identification of the name and location of all supply chain intermediaries between the manufacturer to the contractor to Government acceptance.

(ii) Supply chain traceability documentation shall also include, when available, the manufacturer's batch identification for the item(s), such as date codes, lot codes, or serial numbers. For part numbered items, contractors can find examples of acceptable supply chain traceability documentation at the Counterfeit Detection and Avoidance Program (CDAP) website(https://www.dla.mil/Land-and-Maritime/Business/Selling/Counterfeit-Detection-AvoidanceProgram/).

(iii) In addition, the contractor will obtain, retain, and provide to the contracting officer written documentation of all inspections and tests necessary to substantiate that the supplies furnished under this contract conform to contract requirements, including any applicable technical requirements for specified manufacturers' parts. Such records shall include, without limitation, test reports, test data, material certification, and manufacturing process sheets, in addition to any other information identified in the technical specifications applicable to the item.

(3) The contractor shall make supply chain traceability documentation available to the contracting officer within three business days upon the contracting officer's request. The contracting officer determines the acceptability and sufficiency of documentation. The contractor shall retain supply chain traceability documentation for ten years after final payment under this contract for audit and other valid government purposes. If the contractor fails to retain or provide the documentation, or the contracting officer finds the documentation to be unacceptable, the contracting officer may take corrective action, including, but not limited to, cancellation of undelivered orders or rejection of delivered supplies.

(End of Clause)

Note: An OCONUS delivery order will indicate if C20 Vendor Shipment Module below applies.

C20 Vendor Shipment Module (VSM) (JUN 2025) DLAD

(1) The DLA Vendor Shipment Module (VSM) is a web-based system for DLA contractors to obtain current shipping addresses, two-dimensional bar coded shipping labels in accordance with MILSTD-129, bills of lading, packing lists, and other shipping documentation. Contractors using VSM do not need to contact the transportation office prior to shipping items. Contractors shall use VSM to print labels for f.o.b. destination contracts; and to print labels and arrange for shipping for f.o.b. origin contracts. All contractors will use VSM to obtain shipping labels no more than two (2) days prior to shipment to ensure the current destination address is used.

(2) To obtain information for contracts administered by DLA or to register as a VSM user, the contractor shall contact the DLA VSM Helpdesk at (800) 456-5507 or via email to delivery@dla.mil. (a) Before contacting the Government to advise that material is ready to ship, the contractor shall complete its VSM profile, to include regular business hours and observed holidays. The Government may request reimbursement for occurrences when the Government sends carrier equipment but is unable to pick up a shipment because the material was unavailable, or the contractor facility was closed.

(End of Clause)

Section G – Contract Administration Data

G01 Additional Wide Area Workflow (WAWF) Information (AUG 2017) DLAD

Contractors shall include the Transportation Control Number (TCN) and carrier shipment tracking information when submitting the DD250/iRAPT Receiving Report in Wide Area Workflow (WAWF) in order to assist with material inspection and acceptance.

(End of Clause)

The following provisions and clauses are incorporated by reference:

252.231-7000 Supplemental Cost Principles (DEC 1991) DFARS DEVIATION 2026-O0032
252.232-7003 Electronic Submission of Payment Requests and Receiving Reports (DEC 2018) DFARS DEVIATION 2026-O0022
252.232-7006 Wide Area Workflow Payment Instructions (JAN 2023) DFARS DEVIATION 2026-O0022
Note: 252.232-7006 Fill-ins will be included at the delivery order level.

Section H – Special Contract Requirements

DIN-PACS Program Clauses

DP1 Contract Administration

The Defense Logistics Agency Troop Support is the only organization authorized to administer this contract. Only the DLA Troop Support Contracting Officer can authorize any action at the basic contract level, including contract modifications.

(End of Clause)

DP2 Delivery Order Procedures

Each holder of a current contract under this solicitation and holders of a current contract under SPE2D1-15-R-0004 offering the required supplies shall be provided a fair opportunity consistent with RFO Subparts 16.506 and 16.507, applicable agency acquisition regulation supplements and deviations. Vendors relying on a current contract under SPE2D1-15-R-0004 for eligibility will only be able to compete for orders within that solicitation's scope. Except for unpriced components, offers for a delivery order may only include items on the Contractor's contract at time of award. The evaluation criteria for order selection will be tailored to each requirement, price will always be a factor in order selection. Lowest price technically acceptable or trade-off factors may be used to make delivery order selections. One or more of the following evaluation factors may be used for each order:

A) Price
B) Product features or capabilities
C) Past Performance
D) Warranty and Maintenance features
E) Delivery Timeline
F) Other relevant factors

The ordering of possible factors above does not indicate any relative importance among the factors.

The VA National Acquisition Center (VA NAC), VA Authorized Users, and the Defense Logistics Agency Troop Support (DLA Troop Support) are the only activities currently authorized to place delivery orders under this contract (See Clause 52.216-18 Ordering). The VA NAC, VA Authorized Users, and DLA Troop Support will issue delivery orders directly and process all delivery order administration functions. Any additional ordering authorities may be added at the sole discretion of the DLA Troop Support Contracting Officer, by unilateral modification. Any delegation may be rescinded unilaterally at any time through written notice to vendors. Delivery Orders may support any customer of the ordering authorities, including the Department of Defense, Department of Veterans Affairs, other Federal Agencies/Organizations, and foreign Governments through DoD foreign military sales programs. Agency/Customer specific policies and regulations will be applied at the delivery order level by the issuing agency. VA requirements will be subject to VA policies and regulations while DoD requirements will be subject to DLA and DoD policies and regulations. Delivery Orders executed by VA will incorporate the FAR (and RFO as stipulated in VA-issued deviations) and the correlating VAAR specific clauses.

(End of Clause)

DP3 Modifications (Post-award)

(1) Modification Guidelines: When requesting a modification, including adjustments under the Economic Price Adjustment clause, Contractors shall submit a copy of the Attachment E - Modification Checklist, Attachment F – Modification Price Book, and the other documentation requirements identified in the Modification Checklist or any other information that the Contracting Officer deems necessary. The Contractor may submit requests to modify the contract once per quarter (except in the case of item deletion requests, which follow the procedures in

section DP3(2)(B) below). Failure to provide all of the information required per the Modification Checklist will result in the Contractor's modification request being rejected.

(2) Item Additions/Deletions: In addition to the items that are included in the initial award, the Government may add items to the contract that meet solicitation requirements and are determined to have a fair and reasonable price.

(A) Administration of Additions: The Contractor may submit requests to add items to the contract once per quarter. Any requested additions must be approved by the Contracting Officer before they may be offered under the contract. To be considered, any addition request shall include a completed Attachment A – Vendor Price Book (See Attachment A instructions). Additionally, other than certified cost or pricing data shall be provided that supports the offered pricing. The Contractor shall also provide a certification that all items being added have FDA approvals (when required) and that all items being added have offered pricing that is equal to or better than most favored commercial customers (See Attachment B to this solicitation). The items requested shall go through the same evaluation procedures as items under the initial proposal evaluation. If the Contractor provides insufficient pricing information, the Contracting Officer is authorized to reject the request for additional items. Approval of addition requests shall be implemented by issuance of a contract modification and an updated contract price book.

(B) Item Deletions: At any time during the performance of this contract, the Government may elect to delete any item or items at no cost to the Government. Nonexclusive examples include discovery that the item is not within the solicitation scope, fails to meet contract requirements, or is later found to not have fair and reasonable pricing. Also, at any point during contract performance the Contractor may submit a request to delete items from the contract. All deletions from the contract shall be at no cost to the Government. Vendors will be notified of approval of any deletion requests through issuance of a contract modification and an updated contract price book.

(3) The Government retains the authority to modify the format of the Price Book at any time. Should such a revision occur, the Government shall provide the Contractor notice of the updated format at least 60 days prior to implementing the updated format through unilateral contract modification. Contractors shall submit a new price book in the updated format by the implementation date.

(End of Clause)

DP4 Discontinued Items:

(1) The Contractor shall provide the Government with immediate, written notification when an item is to be discontinued by the manufacturer, including a recommendation for any potential substitute or replacement items.

(2) If an item is discontinued without replacement, the notice should include a recommendation concerning the availability of items that are comparable in form, fit, and function. The contractor shall not incur any costs related to alternate sources of supply without the express written approval of the Contracting Officer. The Government has the option to make a last time order, or series of orders, within 30 days after receiving written notification of the discontinued item after which the item will be deleted from the contract. The Contractor shall honor any last time order unless it is returned to the ordering office within 10 days after issuance, with written notice stating the full quantity is not available for shipment. The terms of such order(s) will be negotiated by the parties, including changes to the delivery schedule and maximum quantity available for shipment.

(End of DIN-PACS Program Clauses)

H11 Section 508 Requirements (OCT 2020) DLAD

Contractors shall comply with the Section 508 Accessibility requirements in this contract and the current revision of the Voluntary Product Accessible Template (VPAT) Rev 508 at DEFENSE LOGISTICS ACQUISITION DIRECTIVE https://www.itic.org/policy/accessibility/vpat (copy website address into browser) as stated in their proposal, for the duration of contract performance.

(End of Clause)

H14 Contractor Personnel Security Requirements (DEC 2021) DLAD

(a) Work to be performed under this contract or task order may, in full or in part, be performed at the Defense Logistics Agency (DLA) Headquarters (HQ), DLA field activity office(s), or other Federally-controlled facilities. Prior to beginning work on a contract, DLA requires all contractor personnel working on the Federally-controlled facility to have, at a minimum, an initiated
National Agency Check with Written Inquiries (NACI) or NACI equivalent and favorable completion of a Federal Bureau of Investigation (FBI) fingerprint check.
(b) Additionally, in accordance with Department of Defense (DoD) Regulation 5200.2-R, Personnel Security Programs, and DLA Issuance 4314, Personnel Security Program, all DoD contractor personnel who have access to Federally-controlled information systems must be assigned to positions which are designated at one of three information technology (IT) levels, each requiring a certain level of investigation and clearance, as follows:

(1) IT-I for an IT position requiring a single scope background investigation (SSBI) or SSBI equivalent;
(2) IT-II for an IT position requiring a National Agency check with Law and Credit (NACLC) or NACLC equivalent; and
(3) IT-III for an IT position requiring a NACI or equivalent.

Note: IT levels will be designated according to the criteria in DoD 5200.2-R.
(c) Previously completed security investigations may be accepted by the Government in lieu of new investigations if determined by the DLA Intelligence Personnel Security Office to be essentially equivalent in scope to the contract requirements. The length of time elapsed since the previous investigation will also be considered in determining whether a new investigation is warranted. To assist the Government in making this determination, the contractor must provide the following information to the respective DLA Intelligence Personnel Security Office immediately upon receipt of the contract. This information must be provided for each contractor employee who will perform work on a Federally-controlled facility and/or will require access to Federally-controlled information systems:

(1) Full name, with middle name, as applicable, with social security number;
(2) Citizenship status with date and place of birth;
(3) Proof of the individual's favorably adjudicated background investigation or NACI, consisting of identification of the type of investigation performed, date of the favorable adjudication, name of the agency that made the favorable adjudication, and name of the agency that performed the investigation;
(4) Company name, address, phone and fax numbers with email address;
(5) Location of on-site workstation or phone number if off-site (if known by the time of award); and
(6) Delivery order or contract number and expiration date; and name of the contracting officer.

(d) The contracting officer will ensure that the contractor is notified as soon as a determination is made by the assigned or cognizant DLA Intelligence Personnel Security Office regarding acceptance of the previous investigation and clearance level.

(1) If a new investigation is deemed necessary, the contractor and contracting officer will be notified by the respective DLA Personnel Security Office after appropriate checks in DoD databases have been made.
(2) If the contractor employee requires access to classified information and currently does not have the appropriate clearance level and/or an active security clearance, the DLA Intelligence Personnel Security Office will relay this information to the contractor and contracting officer for further action. Investigations for contractor employees requiring access to classified information must be initiated by the contractor Facility Security Officer (FSO).

(3) The contracting officer will ensure that the respective DLA Intelligence Personnel Security Office initiates investigations for contractor employees not requiring access to classified information (i.e., IT or unescorted entry).

(4) It is the contractor's responsibility to ensure that adequate information is provided and that each contractor employee completes the appropriate paperwork, as required either by the contracting officer or the DLA Intelligence Personnel Security Office, in order to begin the investigation process for the required clearance level.

(e) The contractor is responsible for ensuring that each contractor employee assigned to the position has the appropriate security clearance level.

(f) The contractor shall submit each request for IT access and investigation through the contracting officer to the assigned or cognizant DLA Intelligence Personnel Security Office. Requests shall include the following information and/or documentation:

(1) Standard Form (SF) 85, Questionnaire for Non-Sensitive Positions, or the SF 86, Questionnaire for National Security Positions (see note below);

(2) Proof of citizenship (i.e., an original or a certified copy of a birth certificate, passport, or naturalization certificate); and

(3) Form FD-258, Fingerprint Card (however, fingerprinting can be performed by the cognizant DLA Intelligence Personnel Security Office).

(Note to (f)(1) above: An investigation request is facilitated through use of the SF 85 or the SF 86. These forms with instructions as well as the Optional Form (OF) 306, Declaration for Federal Employment, which is required with submission of the SF85 or SF 86, are available at the Office of Personnel Management's (OPM) system called Electronic – Questionnaires for Investigations Processing (e-QIP). Hard copies of the SF85 and SF86 are available at OPM's web-site, www.opm.gov, but hard copies of the forms are not accepted.)

(g) Required documentation, listed above in paragraphs (f)(1) through (3), must be provided by the contractor as directed by the contracting officer to the cognizant DLA Intelligence Personnel Security Office at the time of fingerprinting or prior to the DLA Intelligence Personnel Security Office releasing the investigation to OPM.

(h) Upon completion of the NACI, NACLC, SSBI, or other sufficient, appropriate investigation, the results of the investigation will be forwarded by OPM to the appropriate adjudication facility for eligibility determination or the DLA Intelligence Personnel Security Office for review and determination regarding the applicant's suitability to occupy an unescorted entry position in performance of the DLA contract. Contractor personnel shall not commence work on this effort until the investigation has been favorably adjudicated or the contractor employee has been waived into the position pending completion of adjudication. The DLA Intelligence Personnel Security Office will ensure that results of investigations will be sent by OPM to the Department of Defense, Consolidated Adjudications Facility (DoDCAF) or DLA Intelligence Personnel Security Office.

(i) A waiver for IT level positions to allow assignment of an individual contractor employee to commence work prior to completion of the investigation may be granted in emergency situations when it is determined that a delay would be harmful to national security. A request for waiver will be considered only after the Government is in receipt of the individual contractor employee's completed forms, the background investigation has been initiated, and favorable FBI fingerprint check has been conducted. The request for a waiver must be approved by the Commander/Director or Deputy Commander/Director of the site. The cognizant DLA Intelligence Personnel Security Office reserves the right to determine whether a waiver request will be forwarded for processing. The individual contractor employee for which the waiver is being requested may not be assigned to a position, that is, physically work at the Federally-controlled facility and/or be granted access to Federally-controlled information systems, until the waiver has been approved.

(j) The requirements of this procurement note apply to the prime contractor and any subcontractors the prime contractor may employ during the course of this contract, as well as any temporary employees that may be hired by the contractor. The Government retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status whose actions, while assigned to this contract, who are determined by the contracting officer to conflict with the interests of the Government. If such removal occurs, the contractor shall assign qualified personnel, with the required investigation, to any vacancy.

(k) All contractor personnel who are granted access to Government and/or Federally-controlled information systems shall observe all local automated information system (AIS) security policies and procedures. Violations of local AIS security policy, such as password sharing, performing personal work, file access violations, or browsing files outside the scope of the contract, will result in removal of the contractor employee from Government property and referral to the contractor for appropriate disciplinary action. Actions taken by the contractor in response to a violation will be evaluated and will be reflected in the contractor's performance assessment for use in making future source selection decisions. In addition, based on the nature and extent of any violations of AIS security policy, the Government will consider whether it needs to pursue any other actions under the contract such as a possible termination.
(l) The contractor may also be required to obtain a Common Access Card (CAC) or Installation Access Badge for each contractor employee in accordance with procedures established by DLA. When a CAC is required, the contracting officer will ensure that the contractor follows the requirements of Homeland Security Presidential Directive 12 and any other CAC-related requirements in the contract. The contractor shall provide, on a monthly basis, a listing of all personnel working under the contract that have CACs.
(m) See procurement note H16, Operations Security (OPSEC) For On-site Contractors, for required OPSEC training.
(n) When a contractor employee who has been granted a clearance is removed from the contract, the contractor shall provide an appropriately trained substitute who has met or will meet the investigative requirements of this procurement note. The substitute may not begin work on the contract without written documentation, signed by the contracting officer, stating that the new contractor employee has met one of the criteria set forth in paragraphs (c), (d), or (i) of this procurement note (i.e., acceptance of a previously completed security investigation, satisfactory completion of a new investigation, or a waiver allowing work to begin pending completion of an investigation). Contractor individual employees removed from this contract as a result of a violation of local AIS security policy are removed for the duration of the contract.
(o) The following shall be completed for every employee of the Government contractor working on this contract upon contract expiration. Additionally, the contractor shall notify the contracting officer immediately in writing whenever a contractor employee working on this contract resigns, is reassigned, is terminated, or no longer requires admittance to the Federally-controlled facility or access to Federally-controlled information systems. When the contractor employee departs, the contractor will relay departure information to the cognizant DLA Intelligence Personnel Security Office and the Trusted Agent (TA) that entered the individual into the Trusted Associated Sponsorship System (TASS), so appropriate databases can be updated. The contractor will ensure each departed employee has completed the DLA J6 Out-Processing Checklist, when applicable, for the necessary security briefing, has returned any Government furnished equipment, returned the DoD CAC and DLA (or equivalent Installation) badge, returned any DoD or DLA vehicle decal, and requested deletion of local area network account with a prepared Department of Defense (DD) Form 2875. The contractor will be responsible for any costs involved for failure to complete the out-processing, including recovery of Government property and investigation involved.
(p) These contractor security requirements do not excuse the contractor from meeting the delivery schedule/performance requirements set forth in the contract, or waive the delivery schedule/performance requirements in any way. The contractor shall meet the required delivery schedule/performance requirements unless the contracting officer grants a waiver or extension.
(q) The contractor shall not bill for personnel, who are not working on the contract while that contractor employee's clearance investigation is pending.

(End of Clause)

H16 Operations Security (OPSEC) For On-site Contractors (DEC 2021) DLAD

(1) Contractors shall complete the following courses:

(a) Center for the Development of Security Excellence Operations Security (OPSEC) Awareness;
(b) Unauthorized Disclosure of Classified Information for DoD and Industry;
(c) Insider Threat Awareness; and

(d) Introduction to Information Security courses. These courses are located at Security Awareness Hub (https://securityawareness.usalearning.gov/index.html).

(2) The courses identified at subparagraph (1) above are required for all contractors that perform work on-site at a DLA or DoD facility; or for contractors that perform work off-site and access a Federally-controlled information system.

(3) The contractor shall immediately direct its workforce who are performing services for the Government to take the training after contract award. The contractor shall provide evidence of this training to the contracting officer representative or the contracting officer no later than five business days after contract award or prior to accessing the installation or a Federally-controlled information system, whichever occurs first.

(4) Annual refresher training is required and consists of re-accomplishing all of the courses listed in subparagraph (1) above. The contractor shall keep certificates on record for inspection or submission as required by the Government at the Government's discretion.

(End of Clause)

Section I - Contract Clauses

52.252-2 Clauses Incorporated by Reference (FEB 1998) FAR DEVIATION 2026-O0038

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses:

FAR - https://www.acquisition.gov/far-overhaul
DFARS - https://www.acq.osd.mil/dpap/dars/dfars_far_overhaul_class_deviations.html unless noted only with DFARS, then https://www.ecfr.gov/current/title-48/chapter-2
VAAR - https://www.va.gov/oal/library/vaar/vaar852.asp

(End of Clause)

52.252-6 Authorized Deviations in Clauses (NOV 2020) FAR DEVIATION 2026-O0038

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of (DEVIATION) after the date of the clause.
(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation Supplement (48 CFR Chapter 2) clause with an authorized deviation is indicated by the addition of (DEVIATION) after the name of the regulation.
(c) The use in this solicitation or contract of any VA Acquisition Regulation (VAAR) Supplement (48 CFR Chapter 8) clause with an authorized deviation is indicated by the addition of (VAAR DEVIATION) after the name of the regulation.

(End of Clause)

52.212-4 Terms and Conditions Commercial Products and Commercial Services (FEB 2026) FAR DEVIATION 2026-O0038 is incorporated in this solicitation by reference.

The following paragraphs of 52.212-4 are amended as indicated:

1. Paragraph (g), *Invoice*. Electronic invoices shall be used as follows:

Payment Office and Invoicing Instructions for VA Delivery Orders Only:

Contractor shall submit invoices electronically through the Tungsten e-Invoice Network in accordance with VAAR Clause 852.232-72 Electronic Submission of Payment Requests.

The following procedures will apply for all VA NAC Delivery Orders:

(1) The contractor shall send an official e-mail Notification of Delivery and Readiness for Inspection Testing (***after delivery for orders requiring installation***) or Notification of Completion and Readiness for Testing (***after installation or for orders without installation***) to the Contracting Officer (CO). On the notification email, the Contractor shall copy the following personnel, as appropriate, Authorized Customer POC, Technical POC(s), Government Acceptance Testing POC, VA Contracting Officer (CO) and the Biomedical Engineer, along with any others required to be notified as per the instructions in the Delivery Order.

(2) **The contractor shall provide proof of completion for each deliverable(s)** (packing slips, training reports, etc.). This documentation shall be attached to the Tungsten e-Invoice Network submission. The Government will have 30 calendar days to complete the Inspection Testing from the date of the received e-mail notification. The subject line of this e-mail shall be "Installation Completion – Readiness for Inspection Testing Notification" or "Notification of Delivery" when requesting payment. This e-mail shall include the following as a minimum:

(a.) DIN PACS V contract number including Delivery Order number.
(b.) Description of the equipment and/or deliverables to be inspected.
(c.) The Installation Location (Hospital/Facility Name, Room # & Base/City/State).
(d.) Contractor's notification POC information: Name, title, telephone # and e-mail address.
(e.) Contractor's Inspection POC: Name, title, telephone # and e-mail address.

NOTES:

- If the contractor is not subscribed to Tungsten e-Invoice Network, visit https://authentication.tungsten-network.com/login/ and utilize the help links at the bottom of the page.
- Tungsten e-Invoice Network access or input issues should be directed to the Tungsten e-Invoice Network Support.

Payment Office and Invoicing Instructions for VA authorized users (other than VA NAC):

Delivery Orders issued by VA authorized users shall follow local ordering offices' invoices, inspection procedures, and guidance.

Payment Office and Invoicing Instructions for DLA Orders Only: Vendors shall use Wide Area Work Flow (WAWF) for inspection, acceptance and invoicing. The following procedures will apply for all delivery orders:

(1) The vendor shall send an official e-mail Notification of Delivery and Readiness for Inspection Testing (***after delivery for orders requiring installation***) or Notification of Completion and Readiness for Testing (***after installation or for orders without installation***) to PACSNRTI@dla.mil. On the notification email, the Contractor shall copy the Authorized Customer POC, Technical POC(s), Government Acceptance Testing POC and DLA Troop Support Contracting Officer and Biomedical Engineer, noted in the delivery order, along with any others required to be notified as per the instructions in the delivery order. The Government shall have 30 calendar days to complete the Inspection Testing from the date of the e-mail notification. The subject line of this e-mail shall be "Installation Completion – Readiness for Inspection Testing Notification" or "Notification of Delivery" if requesting a commercial interim payment. This e-mail shall include the following as a minimum:

(a.) Complete contract number including delivery order number.
(b.) Description of the equipment and/or CLINs to be inspected.

(c.) The Installation Location (Hospital/Facility Name, Room # & Base/City/State).
(d.) Contractor's notification POC information: Name, title, telephone # and e-mail address.
(e.) Contractor's Inspection POC: Name, title, telephone # and e-mail address.

Vendor is required to provide proof of completion for each CLIN (packing slips, signed acceptance reports, training reports, etc.). This documentation must be attached to the Receiving Report (RR) in WAWF. At a minimum, the vendor shall provide the DD1155, signed by the authorized DoD customer in Block 27, showing that the order lines have been completed (note that the DoD customer is the Requisition POC, who is not necessarily the end-user). Failure to provide the DD1155 may result in rejection of the receiving report and in delays affecting the vendor's ability to invoice the Government. An automated WAWF receiving report submission notification is not sufficient for the above notification requirement

(2) Concurrently with sending of the official e-mail notification, the contractor shall submit a "Material Inspection and Receiving Report" in the form of an "Other/Other Receiving Report (RR) only" in WAWF. ***NOTE: COMBOs cannot be used.***

Critical WAWF Codes for Other/Other Receiving Report:
Pay Office: SL4701
Issue By = SPE2D1
Admin By = Inspect By = Accept at Other = SPE2D1
Ship to: Provided in each delivery order
Errors in critical WAWF codes will result in delayed inspection of the receiving report and may require correction or resubmission prior to processing.

Notes:

- *If Vendor is not subscribed to WAWF, visit https://wawf.eb.mil/ and utilize the help links at the bottom of the page.*
- *WAWF access or input issues should be directed to the Electronic Business Service Desk (1-866-618-5988) or dscpwawfteam@dla.mil.*

(3) The DLA Troop Support engineer shall confirm delivery/inspection with the customer and "Inspect" (digitally sign) the receiving report within 30 calendar days, if no deficiencies are identified.

(4) The DLA Troop Support Contracting Officer shall "Accept" (digitally sign) the receiving report within the same allotted 30 calendar days. The Contracting Officer is the only Government representative who can authorize acceptance in WAWF.

(5) After the Contracting Officer has accepted the receiving report, the vendor shall create and submit an "Invoice Only" from the receiving report in WAWF. This results in a system generated e-mail stating that the invoice has been processed. Upon receipt of the contractor's invoice, payment will be made in accordance with contract terms, NET 30 days. DO NOT SUBMIT AN INVOICE PRIOR TO THE CONTRACTING OFFICER ACCEPTING THE RECEIVING REPORT.

2. Paragraph (i), *Payment.*

DLA Delivery Orders Only:

Delivery cannot occur until authorized by the Contracting Officer, which may be withheld for any failure to comply with contractual/delivery order requirements, including failing to meet cybersecurity requirements.

a. Delivery Orders Requiring Installation:

(1) Delivery orders for equipment/systems requiring installation shall allow a commercial interim payment of 80% of the total price of the equipment/system, in accordance with FAR Part 32. The interim payment will be authorized after a contractor delivers the equipment and the receipt of the equipment is

confirmed by the Contracting Officer (see specific DLA Troop Support receiving, acceptance, and payment requirements/procedures). After acceptance of the contractor's receiving report in WAWF and the contractor has properly submitted an invoice, the 80% interim payment will be processed. The 80% commercial interim payment will be under its own line item.

(2) The remaining 20% of the total price of the equipment/system will be paid after installation has been completed and final inspection and acceptance has occurred. The 20% portion will be under its own line item separate from the commercial interim payment.

(3) Any commercial interim payments are contract financing payments for prompt payment purposes and are not subject to the interest penalty provisions of the Prompt Payment Act in accordance with FAR Subpart 32.9.

b. Delivery Orders without Installation: Delivery orders issued for equipment/systems not requiring installation shall not be eligible for the Commercial Interim Payments.

VA NAC Delivery Orders Only:

Payment shall not be made unless and until it is expressly authorized by the Contracting Officer. The Contracting Officer may withhold authorization for payment in whole or in part in the event of the Contractor's failure to comply with any contractual or Delivery Order requirements, including but not limited to failure to meet applicable cybersecurity obligations.

a. Delivery Orders Requiring Installation:

(1) Delivery orders for equipment/systems requiring installation allow a payment of 80% of the total price of the equipment/system. The payment will be authorized after a contractor delivers the equipment and the receipt of the equipment is confirmed by the Contracting Officer (see specific VA receiving, inspection, acceptance, and payment requirements/procedures). After acceptance of the receiving report and the contractor's submitted proper invoice, the 80% payment will be processed.

(2) The remaining 20% of the total price of the equipment/system will be paid after installation has been completed, all training has been completed, and final inspection and acceptance has been conducted and confirmed by the Contracting Officer.

b. Delivery Orders without Installation: Delivery Orders issued for equipment/systems not requiring installation allow a 100% payment after acceptance has occurred.

VA Authorized Users (other than VA NAC):

These offices shall follow local invoice, receipt of equipment, inspection procedures and guidance.

3. Paragraph (r), *Order of Precedence*. Delete paragraph (r) in its entirety and replace with the following:

Any inconsistency in this request for proposal or contract shall be resolved by giving precedence in the following order:

(a) The Schedule (excluding the specifications).

(b) Representations and other instructions.

(c) Contract clauses.

(d) Other documents, exhibits, and attachments.

(e) The specifications.

(End of Amendments to 52.212-4)

TS 16-08 Economic Price Adjustment – Established Catalog Price - Multiple Adjustments Authorized Per Clause Terms - Non-ECAT (JUN 2017) Troop Support

(a) All price adjustments authorized or mandated by this EPA language are based upon changes in the Contractor's list prices and certain Federal Supply Schedule (FSS) unit prices. The EPA language also provides for voluntary price reductions (VPR) in the form of "specials" or "discounts".

(b) Definitions:

(1) Contract unit price: The price per unit of issue comprised of the "list price" and the applicable "discount". The contract unit price is determined by reducing the applicable list price by the appropriate discount. The list prices and discounts shall be listed in the contract. The resulting net contract unit prices may or may not be listed in the contract at the discretion of the Contracting Officer.

(2) Discount: The percentage reduction off the list price proposed by the Contractor and accepted by the Government. These percentages may vary per item and quantity ordered. They shall be agreed to at time of award and may not be reduced for the life of the contract. These discounts are in addition to any standard trade discounts in the Contractor's established commercial catalog/price list. (Contractors may offer larger discounts and/or reduced list prices at any time.)

(3) List price: The established catalog unit prices of the items. In order for a "list price" to meet the criteria as an established catalog price, it must meet the definition in (c)(1) below.

(4) Voluntary price reduction (VPR): See paragraph (l) below.

(c) Established catalog unit price.

(1) The term "established catalog unit price", as used in this EPA language, means a unit price that (i) is a catalog price for a commercial item sold in substantial quantities to the general public and (ii) is the net price after applying any standard trade discounts offered by the Contractor.

(2) Unless otherwise specified, all reference to the terms "FSS unit price"(s) or "FSS price(s)" as used in this EPA language, shall be the prices appearing in the Contractor's current Federal Supply Schedule for the same items under this contract.

(d) The offeror/Contractor warrants that (1) the list prices and the subsequent revisions thereto are the established catalog unit prices in effect at time of award or adjustment for like quantities of the same items and (2) any contract unit prices determined using these list prices do not include allowances for any portion of the contingency covered by this EPA language. The offeror/Contractor also warrants that any contract unit prices determined using FSS unit prices do not include allowances for any portion of the contingency covered by this EPA language.

(e) Prior to award the Contractor must furnish:

(1) their current established catalog/price list, offered discounts, proposed contract unit prices; and

(2) a copy of their current FSSs, FSS unit prices, and the FSS contract expiration dates applicable to any items offered as well as any other information required by the Contracting Officer.

(f) Upon acceptance by the Government, the award unit prices will be established at the list prices minus the offered discounts provided the resulting contract unit prices do not exceed any current FSS unit price for the same item. Accordingly, offers are cautioned to propose discounts which, when applied to the list prices, will not exceed FSS Unit Prices.

(g) Downward adjustments.

(1) Downward adjustments to contract unit prices are mandated whenever there are decreases in either 1) List Prices or 2) FSS Unit Prices when the reduction results in a revised FSS Price which is now lower than the current Contract Unit Price. The Contractor shall promptly notify the Contracting Officer in writing of the amount and effective date of each decrease in list price and any FSS Unit Price reduction which results in an FSS Unit Price which is now lower than the current Contract Unit Price. If the offered price decrease is based upon a reduction in list price or FSS Price, the Contractor shall propose a lower Contract Unit Price taking into consideration the

benchmarks in paragraphs (g)(2) and (3) below. The Contractor must furnish a copy of the revised Catalog/Price List or FSS Unit Price as soon as it is available. Also, the Contractor must provide an Excel spreadsheet or ACCESS Database (in both hard copy and disc) that displays for each item with an offered decrease in Contract Unit Price the appropriate information below.

For reductions in List Price(s), the Contractor shall submit this information at least 60 days prior to the date when the reduced List Prices take effect. For reductions in FSS Price(s), the Contractor shall provide this information at least 30 days prior to the date the reduced FSS unit price(s) takes effect.

(i) For list price or FSS changes: The item number; e.g., 0001AA.
(ii) For list price or FSS changes: The Supplier (Catalog); e.g., ABC Imaging, Inc.
(iii) For list price or FSS changes: The Product Name/Nomenclature; e.g., High Speed Handpiece.
(iv) For list price or FSS changes: Part Number; e.g., HIH 2000
(v) or list price or FSS changes: The list price upon which the current Contract Unit Price is based.
(vi) For list price or FSS changes: The applicable Contract Discount used as a basis for determining the current Contract Unit Price.
(vii) For list price or FSS changes: The Contract Unit Price currently in effect.
(viii) For list price changes: The reduced List Price.
(ix) For list price changes: The applicable Contract Discount or larger Contract Discount now offered.
(x) For list price or FSS changes: The reduced contract unit price now offered.
(xi) For list price changes: The percentage decrease in list price from the list price which determined the current Contract Unit Price to the new, lower List Price.
(xii) For list price changes: The percentage change in Contract Unit Price from the current Contract Unit Price to the new lower Contract Unit Price now offered.
(xiii) For FSS changes: The current FSS Unit Price which is about to expire and the new reduced FSS Unit Price which will replace it and triggered this Contract Unit Price reduction.
(xiv) For list price changes: For any items offered to the Department of Veterans Affairs (DVA) under the FSS, the current FSS Unit Price(s) for the same item.

(2) Reductions in List Price(s). If the offered price decrease is based upon a reduction in the List Price, the appropriate discount or larger discount now offered will be applied to each reduced list price to determine the adjusted Contract Unit Price provided the proposed lower Contract Unit Price does not exceed the lower of the following two benchmarks:

(i) The offered reduction in Contract Unit Price on a percentage basis must be at least equal to the percentage reduction from the list price currently in effect under the contract to the new lower List Price; i.e., the current Contract Unit Price must, as a minimum, be reduced by the percentage decrease in List Price.
(ii) The new proposed lower Contract Unit Price shall not exceed the current FSS Unit Price for the same item.

(3) FSS Price Reductions. If the offered price decrease is based upon a reduction in the FSS Price, the proposed lower Contract Unit Price shall not exceed the following benchmark: The new proposed lower Contract Unit Price shall not exceed the revised lower FSS Price for the same item.
(4) If the proposed Contract Unit Price exceeds the lower of the appropriate list price benchmarks (for reductions based upon reduced List Prices) or the FSS Price benchmark (for reductions based upon reduced FSS Prices), the Contracting Officer shall determine the proposed price reductions unreasonable and negotiate a price reduction which results in a Contract Unit Price that does not exceed the appropriate benchmarks.

(i) All negotiated price reductions shall be confirmed in writing and will include the agreed-to price(s) and the list price(s) and discount(s) which make up these prices. Changes based upon FSS price reductions will be expressed in terms of the current list price and an appropriate discount which results in an adjusted Contract Unit Price which does not exceed the revised lower FSS Price.
(ii) If an agreement cannot be reached the Contracting Officer has the option of removing these items from the Contract or taking the action in the last sentence below. If the proposed Contract Unit Price does not exceed the lowest of the appropriate list price or FSS Price benchmarks, it will be determined fair and reasonable.

(iii) Upon acceptance of any proposed price decreases, the Government shall modify the contract to include the reduced list prices and discounts (changes based upon FSS price reductions will be expressed in terms of the current list price and an appropriate discount which results in an adjusted Contract Unit Price which does not exceed the revised lower FSS Price). The adjusted contract unit prices may or may not be shown in the modification at the discretion of the Contracting Officer. These reduced contract unit prices shall apply to those items ordered on or after the effective date of the reduced List or FSS Unit Price(s).
(iv) If the Contractor fails to notify the Contracting Officer of any list price or FSS Price decreases within the timeframe and in the manner stated above or agreement on any reduction cannot be reached, the Contracting Officer may determine the applicable adjustment and authorize a unilateral price adjustment retroactively applied to all items ordered on or after the effective date of the decrease in the Contractor's established List or FSS Prices.

(h) Upward Adjustments.

(1) Upward adjustments may be requested at any time. However, any request for upward price adjustment must be based upon increases in List Prices only. The Contractor shall propose a Contract Unit Price taking into consideration the benchmarks in paragraph (g)(2). The request shall include a copy of the revised Catalog/Price List and the following for each item with a proposed increase in Contract Unit Price:

(i) A separate Excel spreadsheet or ACCESS database, in both hard copy and disc, that displays for each item with a proposed price increase the following information:

(A) The item number; e.g., 0003.
(B) The Supplier (Catalog); e.g., ABC Dental, Inc.
(C) The Product Name/Nomenclature; e.g., High Speed Handpiece.
(D) The Part Number; e.g., HIH2000.
(E) For the initial year, the list price that determined the Award Unit Price, the applicable Contract Discount, and the Award Unit Price. For all subsequent contract years, the list price that determined the highest Contract Unit Price that was in effect at any time during the preceding Contract Year, the applicable discount, and the highest Contract Unit Price that was in effect during the preceding Contract Year.
(F) The increased list price and its effective date, the applicable Contract Discount or larger Contract Discount now offered, and the proposed higher Contract Unit Price.
(G) For the initial year, the percentage change from the list price that determined the award unit price to the new higher List Price. For all subsequent contract years, the percentage change from the list price that determined the highest Contract Unit Price that was in effect at any time during the preceding Contract Year to the new higher List Price.
(H) For the initial year, the percentage change from the award unit price to the new higher proposed Contract Unit Price. For all subsequent contract years, the percentage change from the highest Contract Unit Price that was in effect at any time during the preceding contract year to the new higher proposed Contract Unit Price.
(I) For any items offered to the Department of Veterans Affairs (DVA) under the FSS, the current FSS Unit Price(s) for the same item.
(J) Any other information required by the Contracting Officer.

(2) Benchmarks. If any list price increases, and the increase is authorized under this EPA language, the contract unit prices for any corresponding items ordered after the increase takes effect shall be determined using the increased list price and either the applicable Discount originally awarded or any larger Discount now offered that applies to the affected item. Proposed increases will be considered fair and reasonable if they do not exceed whichever is the lowest of the following three benchmarks:

(i) For the Initial Year of the contract, the proposed increase in Contract Unit Price on a percentage basis cannot exceed the percentage increase from the list price that determined the award unit price to the new higher List Price. For all subsequent Contract Years, the proposed increase in Contract Unit Price on a percentage basis cannot exceed the percentage increase from the list price that determined the highest

Contract Unit Price that was in effect at any time during the preceding contract year to the new higher List Price.
(ii) Any proposed higher Contract Unit Price shall not exceed the current FSS Unit Price for the same item.
(iii) Any proposed higher contract unit prices are subject to the following limitations:

(A) For the initial Contract Year, Contract Unit Price increases shall be limited to the following annual ceiling(s) applied to the award unit price for the same item (i.e., any proposed higher Contract Unit Price cannot exceed the award unit price plus the annual ceiling).
(B) For all subsequent Contract Years, Contract Unit Price increases shall be limited to the following annual ceiling(s) applied to the highest Contract Unit Price in effect during the preceding Contract Year for the same item (i.e., any proposed higher Contract Unit Price cannot exceed the highest Contract Unit Price in effect during the preceding Contract Year plus the annual ceiling.)

Annual Ceiling, All Items: 10%

There is no percentage limit on downward adjustments under this EPA language.

(3) Upon approval of the proposed price increases, the Government shall modify the contract to include the increased list prices and discounts. The adjusted contract unit prices may or may not be included in the modification at the discretion of the Contracting Officer.

(i) Upward price adjustments shall be effective within 60 days after receipt of the Contractor's request for upward price adjustment (or at the same time the increased list price takes effect, whichever is later) unless the Contracting Officer is unable to determine during that period that a price increase on any item or items is fair and reasonable (i.e., the proposed Contract Unit Price exceeds the lowest of the three benchmarks above). In this case, no price increases will be authorized for those items until the Contracting Officer is able to determine the price increases for those items to be fair and reasonable. If necessary, the Contracting Officer shall conduct discussions with the Contractor to negotiate a price reduction which results in a Contract Unit Price that does not exceed the lowest of the three benchmarks.
(ii) When discussions have concluded and an agreement which results in fair and reasonable prices is reached, the Contractor shall confirm the agreed-to price(s) in writing (The agreement shall also identify the list price and discount which makes up each agreed-to price.) Once the written agreement is received, the Government shall modify the contract to include the increased list prices and discounts. The adjusted contract unit prices may or may not be included in the modification at the discretion of the Contracting Officer (No increases will be effective prior to the date the increased List Price(s) take effect.)
(iii) If the Contracting Officer and the Contractor are unable to agree upon the price for any items, the Contracting Officer will delete these items from the contract. In addition, the Contracting Officer may also, at any time, remove any item from the contract that the Contracting Officer believes is no longer reasonably priced (if the Contracting Officer and the Contractor are unable to agree upon a reduced price) and notify customers accordingly.

(4) Isolated incidents may occur for an item or group of items when proposed increases could exceed the annual ceiling benchmark in paragraph (h)(2)(iii). In such cases the Contractor can submit an adequately justified written request for Contracting Officer approval of an increase in contract unit price that exceeds the ceiling. The Contracting Officer may approve the request on a one-time basis, increase the ceiling for the item or group of items if appropriate, negotiate a lower contract unit price, or delete the item(s) from the contract. In no case may the increase in Contract Unit Price exceed the ceiling without written authorization from the Contracting Officer. Also, no increase will be authorized that results in a contract unit price that exceeds the other benchmarks.
(5) Any increased list prices shall not be used to compute contract unit prices for delivery orders issued before the date the adjusted contract unit prices take effect under the contract.
(6) If the Contracting Officer removes items from the contract for price unreasonableness (see (g)(4) and (h)(3) and (4) above), all outstanding orders issued prior to the date the items are removed shall be delivered in accordance with the contract delivery schedule and the Government shall pay for such items at the Contract Unit Price in effect at the time of the order.

(i) If the Contracting Officer at any time has any reason to believe that the established list price has been discontinued, the basis for the list price has been substantially altered, or that the item no longer meets the criteria to qualify as an established Catalog Priced item, the Contractor shall furnish relevant information as required by the Contracting Officer. If the Contracting Officer determines that any of the preceding conditions are present and a substitute for determining price adjustments is needed, the parties shall promptly agree upon an appropriate substitute for determining adjustments pursuant to this or other appropriate EPA language. The Contract shall be modified to incorporate the substitute and its effective date.
(j) Pricing actions pursuant to paragraph (c) titled "Changes" of Federal Acquisition Regulation (FAR) clause 52.212-4 (including any revisions by addendum thereto) or any other provision of this Contract will be priced as though there were no provisions for Economic Price Adjustment.
(k) Pending approval of any proposed price changes and the subsequent modification of the contract unit prices, payment shall be made at the contract unit prices in effect at the time of order.
(l) Voluntary Price Reductions (VPR): A "special or discount" offered by the Contractor which results in a voluntary price reduction for an item or group of items for a given period of time. The Contractor may offer a VPR at any time. The price reductions resulting from these VPRs will be in addition to any price reductions mandated by this EPA language.

(1) The Contractor shall notify the Contracting Officer when the VPR takes effect, which items are included, and the length of time the VPR will remain in effect. Once the "special or discount" period expires, prices will revert to the Contract Unit Price(s) in effect at that time.
(2) If a list price (or FSS Unit Price) decreases when a VPR is in effect, the VPR will remain in effect until it expires if it is lower than the proposed unit price decrease. If the Contractor requests a Contract Unit Price increase based upon an increased list price when a VPR is in effect, the VPR shall remain in effect until it expires. Upon expiration of the VPR, prices will revert to the adjusted contract unit prices, as calculated in accordance with this EPA language as if no VPR had been in effect.

(End of Clause)

52.216-18 Ordering (AUG 2020) FAR DEVIATION 2026-O0038

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued from **the date of contract award** through **the last date of the ordering period stated in the contract**.
(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, the contract shall control.
(c) A delivery order or task order is considered "issued" when—
(1) If sent by mail (includes transmittal by U.S. mail or private delivery service), the Government deposits the order in the mail;
(2) If sent by fax, the Government transmits the order to the Contractor's fax number; or
(3) If sent electronically, the Government either—
(i) Posts a copy of the delivery order or task order to a Government document access system, and notice is sent to the Contractor; or
(ii) Distributes the delivery order or task order via email to the Contractor's email address.
(d) Orders may be issued by methods other than those enumerated in this clause only if authorized in the contract.

NOTE: <u>Ordering Activities</u>:

DLA TROOP SUPPORT 700 ROBBINS AVENUE PHILADELPHIA, PA 19111-5092	DEPT. OF VETERANS AFFAIRS NATIONAL ACQUISITION CENTER 1ST AVE. NORTH OFF 22ND BUILDING 37 HINES, IL 60141	DEPT. OF VETERANS AFFAIRS AUTHORIZED USERS

52.216-19 Order Limitations (OCT 1995) FAR DEVIATION 2026-O0038

(a) *Minimum order.* When the Government requires supplies or services covered by this contract in an amount of less than **$1.00**, the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order.* The Contractor is not obligated to honor—

(1) Any order for a single item in excess of **the remaining amount of the contract maximum limitation**;

(2) Any order for a combination of items in excess of **the remaining amount of the contract maximum limitation**; or

(3) A series of orders from the same ordering office within **any number of** days that together call for quantities exceeding the limitation in subparagraph (1) or (2) above.

(c) If this is a requirements contract (i.e., includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR)), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) above.

(d) Notwithstanding paragraphs (b) and (c) above, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within **two** days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

(End of Clause)

52.216-22 Indefinite Quantity (FEB 2026) FAR DEVIATION 2026-O0038

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the “maximum.” The Government shall order at least the quantity of supplies or services designated in the Schedule as the “minimum.”

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order, which may include order options to be exercised after the ordering period of this contract but before the end of the period of performance of the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order, including options exercised, to the same extent as if the order were completed during the contract's ordering period; provided, that the Contractor shall not be required to make any deliveries under this contract after **performance is completed on each delivery order issued under the contract.**

(End of Clause)

52.216-32 Task-Order and Delivery-Order Ombudsman (SEP 2019) Alternate I (SEP 2019) FAR DEVIATION 2026-O0038

(a) In accordance with 41 U.S.C. 4106(g), the Agency has designated the following task-order and delivery-order Ombudsman for this contract. The Ombudsman must review complaints from the Contractor concerning all task-order and delivery-order actions for this contract and ensure the Contractor is afforded a fair opportunity for consideration in the award of orders, consistent with the procedures in the contract.

See paragraph (d).

(b) Consulting an ombudsman does not alter or postpone the timeline for any other process (e.g., protests).

(c) Before consulting with the Ombudsman, the Contractor is encouraged to first address complaints with the Contracting Officer for resolution. When requested by the Contractor, the Ombudsman may keep the identity of the concerned party or entity confidential, unless prohibited by law or agency procedure.
(d) Contracts used by multiple agencies.

(1) This is a contract that is used by multiple agencies. Complaints from Contractors concerning orders placed under contracts used by multiple agencies are primarily reviewed by the task-order and delivery-order Ombudsman for the ordering activity.

(2) The ordering activity has designated the following task-order and delivery-order Ombudsman for this order:

DLA Troop Support:

DLA Troop Support Competition Advocate, BPA
700 Robbins Avenue
Philadelphia, PA 19111-5096

VA NAC and Authorized VA Users: AcquisitionRMCS@va.gov.

NOTE: Please send a full description of your complaint along with relevant order information, such as task or delivery order number, IDIQ contract number, solicitation number, and name of contracting officer to AcquisitionRMCS@va.gov.

(3) Before consulting with the task-order and delivery-order Ombudsman for the ordering activity, the Contractor is encouraged to first address complaints with the ordering activity's Contracting Officer for resolution. When requested by the Contractor, the task-order and delivery-order Ombudsman for the ordering activity may keep the identity of the concerned party or entity confidential, unless prohibited by law or agency procedure.

(End of Clause)

Note: 52.217-9 below applies to resultant basic contracts awarded within five years of the solicitation issue date.

52.217-9 Option to Extend the Term of the Contract (MAR 2000) FAR DEVIATION 2026-O0038

a) The Government may extend the term of this contract by written notice to **the Contractor at any time before the first day after the base term ordering period**; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least **60** days before **the first day after the base term ordering period.** The preliminary notice does not commit the Government to an extension.
(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.
(c) The **total ordering period of this contract**, including the exercise of any options under this clause, shall not exceed **10 years**.

52.229-11 Tax on Certain Foreign Procurements—Notice and Representation (FEB 2026) FAR DEVIATION 2026-O0038

(a) *Definitions*. As used in this provision—

Foreign person means any person other than a United States person.

Specified Federal procurement payment means any payment made pursuant to a contract with a foreign contracting party that is for goods, manufactured or produced, or services provided in a foreign country that is not a party to an international procurement agreement with the United States. For purposes of the prior sentence, a foreign country does not include an outlying area of the United States.

United States person as defined in 26 U.S.C. 7701(a)(30) means

(1) A citizen or resident of the United States;

(2) A domestic partnership;

(3) A domestic corporation;

(4) Any estate (other than a foreign estate, within the meaning of 26 U.S.C. 701(a)(31)); and

(5) Any trust if–

(i) A court within the United States is able to exercise primary supervision over the administration of the trust; and

(ii) One or more United States persons have the authority to control all substantial decisions of the trust.

(b) Unless exempted, there is a 2 percent tax of the amount of a specified Federal procurement payment on any foreign person receiving such payment. See 26 U.S.C. 5000C and its implementing regulations at 26 CFR 1.5000C-1 through 1.5000C-7.

(c) Exemptions from withholding under this provision are described at 26 CFR 1.5000C-1(d)(5) through (7). The Offeror may claim an exemption from the withholding by using the Department of the Treasury Internal Revenue Service (IRS) Form W-14, Certificate of Foreign Contracting Party Receiving Federal Procurement Payments, available at www.irs.gov/w14. Any exemption claimed and self-certified on the IRS Form W-14 is subject to audit by the IRS. Any disputes regarding the imposition and collection of the 26 U.S.C. 5000C tax are adjudicated by the IRS as the 26 U.S.C. 5000C tax is a tax matter, not a contract issue. The IRS Form W-14 is provided to the acquiring agency rather than to the IRS.

(d) For purposes of withholding under 26 U.S.C. 5000C, the Offeror represents that

(1) It **[_]** is **[_]** is not a foreign person; and

(2) If the Offeror indicates "is" in paragraph (d)(1) of this provision, then the Offeror represents that—I am claiming on the IRS Form W-14 **[_]** a full exemption, or **[_]** partial or no exemption [Offeror must select one] from the excise tax.

(e) If the Offeror represents it is a foreign person in paragraph (d)(1) of this provision, then—

(1) The clause at FAR 52.229-12, Tax on Certain Foreign Procurements, will be included in any resulting contract; and

(2) The Offeror shall submit with its offer the IRS Form W-14. If the IRS Form W-14 is not submitted with the offer, exemptions will not be applied to any resulting contract and the Government will withhold a full 2 percent of each payment.

(f) If the Offeror selects "is" in paragraph (d)(1) and "partial or no exemption" in paragraph (d)(2) of this provision, the Offeror will be subject to withholding in accordance with the clause at FAR 52.229-12, Tax on Certain Foreign Procurements, in any resulting contract.

(g) A taxpayer may, for a fee, seek advice from the IRS as to the proper tax treatment of a transaction. This is called a private letter ruling. Also, the IRS may publish a revenue ruling, which is an official interpretation by the IRS of the Internal Revenue Code, related statutes, tax treaties, and regulations. A revenue ruling is the conclusion of the IRS on how the law is applied to a specific set of facts. For questions relating to the interpretation of the IRS regulations go to https://www.irs.gov/help/tax-law-questions.

(End of provision)

852.211-76 Liquidated Damages—Reimbursement for Data Breach Costs (FEB 2023) VAAR – VA Delivery Orders Only.

(a) Definition. As used in this clause, "contract" means any contract, agreement, order or other instrument and encompasses the definition set forth in FAR 2.101.

(b) Non-disclosure requirements. As a condition of performance under a contract, order, agreement, or other instrument that requires access to sensitive personal information as defined in VAAR 802.101, the following is expressly required—

(1) The Contractor, subcontractor, their employees or business associates shall not, directly or through an affiliate or employee of the Contractor, subcontractor, or business associate, disclose sensitive personal information to any other person unless the disclosure is lawful and is expressly permitted under the contract; and

(2) The Contractor, subcontractor, their employees or business associates shall immediately notify the Contracting Officer and the Contracting Officer's Representative (COR) of any security incident that occurs involving sensitive personal information.

(c) Liquidated damages. If the Contractor or any of its agents fails to protect VA sensitive personal information or otherwise engages in conduct which results in a data breach, the Contractor shall, in place of actual damages, pay to the Government liquidated damages of $51.38 per affected individual in order to cover costs related to the notification, data breach analysis and credit monitoring. In the event the Contractor provides payment of actual damages in an amount determined to be adequate by the Contracting Officer, the Contracting Officer may forgo collection of liquidated damages.

(d) Purpose of liquidated damages. Based on the results from VA's determination that there was a data breach caused by Contractor's or any of its agents' failure to protect or otherwise engaging in conduct to cause a data breach of VA sensitive personal information, and as directed by the Contracting Officer, the Contractor shall be responsible for paying to the VA liquidated damages in the amount of $51.38 per affected individual to cover the cost of the following:

(1) Notification related costs.

(2) Credit monitoring reports.

(3) Data breach analysis and impact.

(4) Fraud alerts.

(5) Identity theft insurance.

(e) Relationship to termination clause, if applicable. If the Government terminates this contract, purchase order, or agreement, in whole or in part under clause 52.249-8, Default—Fixed-Price Supply and Service, or any other related FAR or VAAR clause included in the contract, in addition to the required liquidated damages for data breach-related expenses specified in paragraph (c) above, the Contractor is liable for excess costs for those supplies and services for repurchase as may be required under the Termination clause.

(End of clause)

Alternate I (FEB 2023). In commercial products or commercial services acquisitions awarded under the procedures of FAR part 8 or 12, substitute this paragraph (e) in lieu of paragraph (e) in the basic clause:

(e) Relationship to termination clause, if applicable. If the Government terminates this contract in whole or in part under the Termination for cause paragraph, FAR 52.212-4(m), Terms and Conditions—Commercial Products and Commercial Services, the Contractor is liable for damages accruing until the Government reasonably obtains

delivery or performance of similar supplies or services. These damages are in addition to costs of repurchase as may be required under the Termination clause.

Delay of Installation for Medical and Laboratory Instrumentation – DLA– Troop Support – Medical

(a) Installation (reference installation clause at SOW Appendix 3, above) shall not commence until authorized by the chief of medical materiel services (CMMS) at the hospital. It shall be the Contractor's responsibility to inform the CMMS with information copy to the Contracting Officer, of any problems which may be anticipated in connection with installation or which will adversely affect performance once installation is completed. Such matters as inadequacy of power supply, limitations of site, or inadequate preparation of site shall be included in information reported prior to start of installation. Installation shall not proceed under such circumstances until notified by the CMMS at the hospital, with information copy to the Contracting Officer.
(b) Unless otherwise authorized by the Contracting Officer, installation of the system/equipment shall in no event exceed * calendar days from the date of notice to proceed with installation.
(c) In the event that progress in the installation is interrupted through no fault of the Contractor, the continuous installation referred to in the installation clause may be terminated until such time as the cause of delay has been eliminated, and then shall be resumed within 24 hours after the Contractor has been notified by the CMMS that work may again proceed. (Except in those situations where life and/or property would be imperiled by such delay, termination of installation shall be made only after 2 hours' notice has been given to CMMS at the hospital receiving installation.)

*The number of calendar days will be established in the delivery order.

(End of Clause)

Additional clauses incorporated by reference:

52.203-3 Gratuities (APR 1984) FAR DEVIATION 2026-O0038
52.203-6 Restrictions on Subcontractor Sales to the Government (JUN 2020) Alternate I (NOV 2021) FAR DEVIATION 2026-O0038
52.203-13 Contractor Code of Business Ethics and Conduct (NOV 2021) FAR DEVIATION 2026-O0038
52.203-17 Contractor Employee Whistleblower Rights (NOV 2023) FAR (VAAR DEVIATION NOV 2025)– VA Delivery Orders Only
52.203-19 Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (JAN 2017) FAR DEVIATION 2026-O0038
252.203-7000 Requirements Relating to Compensation of Former DoD Officials (SEP 2011) DFARS DEVIATION 2026-O0031
252.203-7002 Requirement to Inform Employees of Whistleblower Rights (DEC 2022) DFARS DEVIATION 2026-O0031
52.204-9 Personal Identity Verification of Contractor Personnel (JAN 2011) FAR DEVIATION 2026-O0043
52.204-13 System for Award Management Maintenance (FEB 2026) FAR DEVIATION 2026-O0043
252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (MAY 2024) DFARS DEVIATION 2026-O0025 Revision 2 and DEVIATION 2024-O0013 Revision 1
252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services (JAN 2023) DFARS DEVIATION 2026-O0025 Revision 2
252.240-7997 NIST SP 800-171 DoD Assessment Requirements (FEB 2026) DFARS DEVIATION 2026-O0025 Revision 2
252.205-7000 Provision of Information to Cooperative Agreement Holders (OCT 2024) DFARS DEVIATION 2026-O0003
52.209-6 Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (FEB 2026) FAR DEVIATION 2026-O0038
52.209-9 Updates of Publicly Available Information Regarding Responsibility Matters (FEB 2026) FAR DEVIATION 2026-O0038
52.209-10 Prohibition on Contracting with Inverted Domestic Corporations (FEB 2026) FAR DEVIATION 2026-O0038

252.209-7004 Subcontracting with Firms that are Owned or Controlled by the Government of a Country that is a State Sponsor of Terrorism (MAY 2019) DFARS DEVIATION 2026-O0042
252.211-7003 Item Unique Identification and Valuation (JAN 2023) DFARS DEVIATION 2026-O0013
252.211-7008 Use of Government-Assigned Serial Numbers (SEP 2010) DFARS DEVIATION 2026-O0013
52.215-21 Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data—Modifications (FEB 2026) FAR DEVIATION 2026-O0038
252.215-7992 Only One Offer (MAR 2026) DFARS DEVIATION 2026-O0048
NOTE: 252.215-7992 applies at the delivery order level
252.216-7010 Postaward Debriefings for Task Orders and Delivery Orders (OCT 2025) DFARS DEVIATION 2026-O0045 Revision 1
52.219-8 Utilization of Small Business Concerns (FEB 2026) FAR DEVIATION 2026-O0038
52.219-9 Small Business Subcontracting Plan (FEB 2026) Alternate II (FEB 2026) FAR DEVIATION 2026-O0038
52.219-16 Liquidated Damages—Subcontracting Plan (FEB 2026) FAR DEVIATION 2026-O0038
252.219-7996 Small Business Subcontracting Plan (DoD Contracts) – Basic (FEB 2026) DFARS DEVIATION 2026-O0037
52.222-35 Equal Opportunity for Veterans (FEB 2026) FAR DEVIATION 2026-O0038
52.222-36 Equal Opportunity for Workers with Disabilities (FEB 2026) FAR DEVIATION 2026-O0038
52.222-37 Employment Reports on Veterans (FEB 2026) FAR DEVIATION 2026-O0038
52.222-40 Notification of Employee Rights Under the National Labor Relations Act (FEB 2026) FAR DEVIATION 2026-O0038
52.222-50 Combating Trafficking in Persons (FEB 2026) FAR DEVIATION 2026-O0038
52.222-51 Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment—Requirements (FEB 2026) FAR DEVIATION 2026-O0038
52.222-90 Addressing DEI Discrimination by Federal Contractors (APR 2026) FAR DEVIATION 2026-O0038
52.223-3 Hazardous Material Identification and Material Safety Data (FEB 2026) FAR DEVIATION 2026-O0038
52.223-23 Sustainable Products and Services (FEB 2026) FAR DEVIATION 2026-O0038
NOTE: 52.223-23 Does not apply to supplies delivered outside the United States
252.223-7001 Hazard Warning Labels (DEC 1991) DFARS DEVIATION 2026-O0018
252.223-7008 Prohibition of Hexavalent Chromium (JAN 2023) DFARS DEVIATION 2026-O0018
52.224-1 Privacy Act Notification (APR 1984) FAR DEVIATION 2026-O0038
52.224-2 Privacy Act (APR 1984) FAR DEVIATION 2026-O0038
52.224-3 Privacy Training (JAN 2017) Alternate I (JAN 2017) FAR DEVIATION 2026-O0038
NOTE: For DLA delivery orders, the application of Alternate I and additional Privacy Act requirements will be determined at the delivery order level. Privacy Act training is distinct from other security training requirements.
252.225-7012 Preference for Certain Domestic Commodities (APR 2022) DFARS DEVIATION 2026-O0041 Revision 1
252.225-7015 Restriction on Acquisition of Hand or Measuring Tools (JUN 2005) DFARS DEVIATION 2026-O0041 Revision 1
252.225-7021 Trade Agreements-Basic (FEB 2024) DFARS DEVIATION 2026-O0041 Revision 1
252.225-7052 Restrictions on the Acquisition of Certain Magnets, Tantalum and Tungsten (MAY 2024) DFARS DEVIATION 2026-OO0041 Revision 1
252.225-7056 Prohibition Regarding Business Operations with the Maduro Regime (JAN 2023) DFARS DEVIATION 2026-O0041 Revision 1
252.225-7060 Prohibition on Certain Procurements from the Xinjiang Uyghur Autonomous Region (JUN 2023) DFARS DEVIATION 2026-O0041 Revision 1
252.225-7962 Threat Mitigation Support to Operations. (JUN 2026) DFARS DEVIATION 2026-O0051
252.225-7967 Prohibition Regarding Russian Fossil Fuel Business Operations (FEB 2024) DEVIATION 2024-O0006, Revision 1
252.225-7975 Additional Access to Contractor and Subcontractor Records. (JUN 2026) DFARS DEVIATION 2026-O0051
52.226-8 Encouraging Contractor Policies to Ban Text Messaging While Driving (May 2024) FAR DEVIATION 2026-O0038
252.226-7001 Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns (JAN 2023) DFARS DEVIATION 2026-O0008

52.227-1 Authorization and Consent (JUN 2020) FAR DEVIATION 2026-O0038
52.227-2 Notice and Assistance Regarding Patent and Copyright Infringement (JUN 2020) FAR DEVIATION 2026-O0038
252.227-7990 Technical Data – Commercial Products and Commercial Services (FEB 2026) DFARS DEVIATION 2026-O0036
252.227-7997 Validation of Asserted Restrictions on Technical Data (FEB 2026) DFARS DEVIATION 2026-O0036
52.229-12 Tax on Certain Foreign Procurements (FEB 2026) FAR DEVIATION 2026-O0038
252.229-7012 Tax Exemptions (Italy)—Representation (MAR 2012) DEVIATION 2026-O0007
NOTE: 252.229-7012 will only apply to orders requiring delivery in Italy, its completion is not required with the initial offer.
252.229-7013 Tax Exemptions (Spain)—Representation (APR 2012) DEVIATION 2026-O0007
NOTE: 252.229-7013 will only apply to orders requiring delivery in Spain, its completion is not required with the initial offer.
252.229-7014 Full Exemption from Two-Percent Tax on Certain Foreign Procurements (OCT 2022) DFARS DEVIATION 2026-O0007
52.232-33 Payment by Electronic Funds Transfer—System for Award Management (OCT 2018) FAR DEVIATION 2026-O0038
52.232-40 Providing Accelerated Payments to Small Business Subcontractors (MAR 2023) FAR DEVIATION 2026-O0038
252.232-7010 Levies on Contract Payments (DEC 2006) DFARS DEVIATION 2026-O0022
52.233-3 Protest After Award (FEB 2026) FAR DEVIATION 2026-O0038
52.233-4 Applicable Law for Breach of Contract Claim (FEB 2026) FAR DEVIATION 2026-O0038
252.239-7018 Supply Chain Risk (DEC 2022) DFARS DEVIATION 2026-O0025 Revision 2
52.240-91 Security Prohibitions and Exclusions (FEB 2026) FAR DEVIATION 2026-O0038
52.240-93 Basic Safeguarding of Covered Contractor Information Systems (FEB 2026) FAR DEVIATION 2026-O0038
52.242-5 Payments to Small Business Subcontractors (JAN 2017) FAR DEVIATION 2026-O0038
52.242-13 Bankruptcy (July 1995) FAR DEVIATION 2026-O0038
252.243-7001 Pricing of Contract Modifications (DEC 1991) DFARS DEVIATION 2026-O0034
252.243-7002 Requests for Equitable Adjustment (DEC 2022) DFARS DEVIATION 2026-O0034
252.244-7999 Subcontracts for Commercial Products or Commercial Services (FEB 2026) DFARS DEVIATION 2026-O0015
252.246-7003 Notification of Potential Safety Issues (JAN 2023) DFARS DEVIATION 2026-O0035
252.246-7007 Contractor Counterfeit Electronic Part Detection and Avoidance System (JAN 2023) DFARS DEVIATION 2026-O0035
252.246-7008 Sources of Electronic Parts (JAN 2023) DFARS DEVIATION 2026-O0035
252.247-7023 Transportation of Supplies by Sea (OCT 2024) DFARS DEVIATION 2026-O0047
852.203-70 Commercial Advertising (MAY 2018) VAAR – Basic Contract and VA Delivery Orders
852.204-70 Personal Identity Verification of Contractor Personnel (MAY 2020) VAAR – VA Delivery Orders Only
852.204-71 Information and Information Systems Security (FEB 2023) VAAR – VA Delivery Orders Only
852.232-72 Electronic Submission of Payment Requests (NOV 2018) VAAR DEVIATION MAR 2026) – VA Delivery Orders Only

The following clauses will only apply to delivery orders requiring delivery in the country indicated in the clause.

252.225-7976 Contractor Personnel Performing in Japan (AUG 2018) DFARS DEVIATION 2018-O0019
252.229-7002 Customs Exemptions (Germany) (JUN 1997) DFARS DEVIATION 2026-O0007
252.229-7003 Tax Exemptions (Italy) (MAR 2012) DFARS DEVIATION 2026-O0007
252.229-7005 Tax Exemptions (Spain) (MAR 2012) DFARS DEVIATION 2026-O0007
252.229-7006 Value Added Tax Exclusion (United Kingdom) (DEC 2011) DFARS DEVIATION 2026-O0007
252.229-7007 Verification of United States Receipt of Goods (JUN 1997) DFARS DEVIATION 2026-O0007

Section J - List of Attachments

Attachment A – Vendor Price Book
Attachment B – Price and Discount Information
Attachment C – Offeror Exceptions to Terms and Conditions
Attachment D – Statement of Work Responses
Attachment E – Modification Check List
Attachment F – Modification Spreadsheet
Attachment G – VA Handbook 6500.6 Appendix A – Checklist for Information Security in the Initiation Phase of Acquisitions
Attachment H – VA Directive 6550 Appendix A

Section K – Representations, Certification, and Other Statements of Offerors

252.204-7016 Covered Defense Telecommunications Equipment or Services—Representation (DEC 2019) DFARS DEVIATION 2026-O0025 Revision 2

(a) Definitions. As used in this provision, "covered defense telecommunications equipment or services" has the meaning provided in the clause 252.204-7018, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services.

(b) Procedures. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) (https://www.sam.gov) for entities excluded from receiving federal awards for "covered defense telecommunications equipment or services".

(c) Representation. The Offeror represents that it [ ] does, [ ] does not provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument.

(End of Provision)

252.204-7017 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services—Representation (MAY 2021) DFARS DEVIATION 2026-O0025 Revision 2

The Offeror is not required to complete the representation in this provision if the Offeror has represented in the provision at 252.204-7016, Covered Defense Telecommunications Equipment or Services—Representation, that it "does not provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument."

(a) *Definitions*. "Covered defense telecommunications equipment or services," "covered mission," "critical technology," and "substantial or essential component," as used in this provision, have the meanings given in the 252.204-7018 clause, Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services, of this solicitation.

(b) *Prohibition*. Section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits agencies from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(c) *Procedures*. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at *https://www.sam.gov* for entities that are excluded when providing any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless a waiver is granted.

(d) *Representation*. If in its annual representations and certifications in SAM the Offeror has represented in paragraph (c) of the provision at 252.204-7016, Covered Defense Telecommunications Equipment or Services—Representation, that it "does" provide covered defense telecommunications equipment or services as a part of its offered products or services to the Government in the performance of any contract, subcontract, or other contractual instrument, then the Offeror shall complete the following additional representation:

The Offeror represents that it [ ] will [ ] will not provide covered defense telecommunications equipment or services as a part of its offered products or services to DoD in the performance of any award resulting from this solicitation.

(e) *Disclosures*. If the Offeror has represented in paragraph (d) of this provision that it "will provide covered defense telecommunications equipment or services," the Offeror shall provide the following information as part of the offer:

(1) A description of all covered defense telecommunications equipment and services offered (include brand or manufacturer; product, such as model number, original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable).

(2) An explanation of the proposed use of covered defense telecommunications equipment and services and any factors relevant to determining if such use would be permissible under the prohibition referenced in paragraph (b) of this provision.

(3) For services, the entity providing the covered defense telecommunications services (include entity name, unique entity identifier, and Commercial and Government Entity (CAGE) code, if known).

(4) For equipment, the entity that produced or provided the covered defense telecommunications equipment (include entity name, unique entity identifier, CAGE code, and whether the entity was the OEM or a distributor, if known).

(End of provision)

52.209-7 - Information Regarding Responsibility Matters (FEB 2026) FAR DEVIATION 2026-O0038

(a) *Definitions*. As used in this provision—

Administrative proceeding means a non-judicial process that is adjudicatory in nature in order to make a determination of fault or liability (e.g., Securities and Exchange Commission Administrative Proceedings, Civilian Board of Contract Appeals Proceedings, and Armed Services Board of Contract Appeals Proceedings). This includes administrative proceedings at the Federal and State level but only in connection with performance of a Federal contract or grant. It does not include agency actions such as contract audits, site visits, corrective plans, or inspection of deliverables.

Federal contracts and grants with total value greater than $10,000,000 means—

(1) The total value of all current, active contracts and grants, including all priced options; and

(2) The total value of all current, active orders including all priced options under indefinite-delivery, indefinite-quantity, 8(a), or requirements contracts (including task and delivery and multiple-award Schedules).

Principal means an officer, director, owner, partner, or a person having primary management or supervisory responsibilities within a business entity (e.g., general manager; plant manager; head of a division or business segment; and similar positions).

(b) The offeror [ ] has [ ] does not have current active Federal contracts and grants with total value greater than $10,000,000.

(c) If the offeror checked "has" in paragraph (b) of this provision, the offeror represents, by submission of this offer, that the information it has entered in the Federal Awardee Performance and Integrity Information System (FAPIIS) is current, accurate, and complete as of the date of submission of this offer with regard to the following information:

(1) Whether the offeror, and/or any of its principals, has or has not, within the last five years, in connection with the award to or performance by the offeror of a Federal contract or grant, been the subject of a proceeding, at the Federal or State level that resulted in any of the following dispositions:

(i) In a criminal proceeding, a conviction.

(ii) In a civil proceeding, a finding of fault and liability that results in the payment of a monetary fine, penalty, reimbursement, restitution, or damages of $5,000 or more.

(iii) In an administrative proceeding, a finding of fault and liability that results in—

(A) The payment of a monetary fine or penalty of $5,000 or more; or

(B) The payment of a reimbursement, restitution, or damages in excess of $100,000.

(iv) In a criminal, civil, or administrative proceeding, a disposition of the matter by consent or compromise with an acknowledgment of fault by the Contractor if the proceeding could have led to any of the outcomes specified in paragraphs (c)(1)(i), (c)(1)(ii), or (c)(1)(iii) of this provision.

(2) If the offeror has been involved in the last five years in any of the occurrences listed in (c)(1) of this provision, whether the offeror has provided the requested information with regard to each occurrence.

(d) The offeror shall post the information in paragraphs (c)(1)(i) through (c)(1)(iv) of this provision in FAPIIS as required through maintaining an active registration in the System for Award Management, which can be accessed via https://www.sam.gov (see 52.204-7).

(End of provision)

52.209-12 Certification Regarding Tax Matters (OCT 2025) FAR DEVIATION 2026-O0038

(a) This provision implements section 523 of Division B of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235), and similar provisions, if contained in subsequent appropriations acts.

(b) If the Offeror is proposing a total contract price that will exceed $7 million (including options), the Offeror shall certify that, to the best of its knowledge and belief, it

(1) Has [_] filed all Federal tax returns required during the three years preceding the certification;

(2) Has not [_] been convicted of a criminal offense under the Internal Revenue Code of 1986; and

(3) Has not [_], more than 90 days prior to certification, been notified of any unpaid Federal tax assessment for which the liability remains unsatisfied, unless the assessment is the subject of an installment agreement or offer in compromise that has been approved by the Internal Revenue Service and is not in default, or the assessment is the subject of a non-frivolous administrative or judicial proceeding.

(End of provision)

52.222-18 Certification Regarding Knowledge of Child Labor for Listed End Products (Feb 2021) FAR DEVIATION 2026-O0038

(a) *Definition*.

Forced or indentured child labor means all work or service-

(1) Exacted from any person under the age of 18 under the menace of any penalty for its nonperformance and for which the worker does not offer himself voluntarily; or

(2) Performed by any person under the age of 18 pursuant to a contract the enforcement of which can be accomplished by process or penalties.

(b) *Listed end products*. The following end product(s) being acquired under this solicitation is (are) included in the List of Products Requiring Contractor Certification as to Forced or Indentured Child Labor, identified by their country of origin. There is a reasonable basis to believe that listed end products from the listed countries of origin may have been mined, produced, or manufactured by forced or indentured child labor.

Listed End Product	**Listed Countries of Origin**
Electronics	China

(c) Certification. The Government will not make award to an offeror unless the offeror, by checking the appropriate block, certifies to either paragraph (c)(1) or paragraph (c)(2) of this provision.

[__] (1) The offeror will not supply any end product listed in paragraph (b) of this provision that was mined, produced, or manufactured in a corresponding country as listed for that end product.

[__] (2) The offeror may supply an end product listed in paragraph (b) of this provision that was mined, produced, or manufactured in the corresponding country as listed for that product. The offeror certifies that it has made a good faith effort to determine whether forced or indentured child labor was used to mine, produce, or manufacture such end product. On the basis of those efforts, the offeror certifies that it is not aware of any such use of child labor.

(End of provision)

52.222-48 Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Certification (FEB 2026) FAR DEVIATION 2026-O0038

(a) The offeror must check the following certification:

Certification

The offeror [_] does [_] does not certify that-

(1) The items of equipment to be serviced under this contract are used regularly for other than Government purposes, and are sold or traded by the offeror (or subcontractor in the case of an exempt subcontractor) in substantial quantities to the general public in the course of normal business operations;

(2) The services will be furnished at prices which are, or are based on, established catalog or market prices for the maintenance, calibration, or repair of equipment.

(i) An "established catalog price" is a price included in a catalog, price list, schedule, or other form that is regularly maintained by the manufacturer or the offeror, is either published or otherwise available for inspection by customers, and states prices at which sales currently, or were last, made to a significant number of buyers constituting the general public.

(ii) An "established market price" is a current price, established in the usual course of trade between buyers and sellers free to bargain, which can be substantiated from sources independent of the manufacturer or offeror; and

(3) The compensation (wage and fringe benefits) plan for all service employees performing work under the contract are the same as that used for these employees and equivalent employees servicing the same equipment of commercial customers.

(b) Certification by the offeror as to its compliance with respect to the contract also constitutes its certification as to compliance by its subcontractor if it subcontracts out the exempt services. If the offeror certifies to the conditions in paragraph (a) of this provision, and the Contracting Officer determines in accordance with FAR 22.1002-1(e)(3) that the Service Contract Labor Standards statute-

(1) Will not apply to this offeror, then the Service Contract Labor Standards clause in this solicitation will not be included in any resultant contract to this offeror; or

(2) Will apply to this offeror, then the clause at 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements, in this solicitation will not be included in any resultant contract awarded to this offeror, and the offeror may be provided an opportunity to submit a new offer on that basis.

(c) If the offeror does not certify to the conditions in paragraph (a) of this provision-

(1) The clause in this solicitation at 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment-Requirements, will not be included in any resultant contract awarded to this offeror; and

(2) The offeror must notify the Contracting Officer as soon as possible, if the Contracting Officer did not attach a Service Contract Labor Standards wage determination to the solicitation.

(d) The Contracting Officer may not make an award to the offeror, if the offeror fails to execute the certification in paragraph (a) of this provision or to contact the Contracting Officer as required in paragraph (c) of this provision.

(End of provision)

252.225-7020 - Trade Agreements Certificate (NOV 2014) DEVIATION 2026-O0041

(a) *Definitions.* “Designated country end product,” “nondesignated country end product,” “qualifying country end product,” and “U.S.-made end product” as used in this provision have the meanings given in the Trade Agreements—Basic clause of this solicitation.

(b) *Evaluation.* The Government—

(1) Will evaluate offers in accordance with the policies and procedures of Part 225 of the Defense Federal Acquisition Regulation Supplement; and

(2) Will consider only offers of end products that are U.S.-made, qualifying country, or designated country end products unless—

(i) There are no offers of such end products;

(ii) The offers of such end products are insufficient to fulfill the Government's requirements; or

(iii) A national interest waiver has been granted.

(c) *Certification and identification of country of origin.*

(1) For all line items subject to the Trade Agreements—Basic clause of this solicitation, the offeror certifies that each end product to be delivered under this contract, except those listed in paragraph (c)(2) of this provision, is a U.S.-made, qualifying country, or designated country end product.

(2) The following supplies are other nondesignated country end products:

Line Item Number	Country of Origin

[List as necessary]

(End of Provision)

252.225-7966 Prohibition Regarding Russian Fossil Fuel Business Operations—Representation (DEVIATION 2024-O0006, Revision 1) (MAR 2024).

(a) Definitions. The terms business operations and fossil fuel company have the meanings given in the 252.225-7967 clause of this solicitation.

(b) Representation. By submission of an offer, the Offeror represents it is not, or that it does not knowingly have fossil fuel business operations with an entity or individual that is, 50 percent or more owned, individually or collectively, by—

(1) An authority of the government of the Russian Federation; or
(2) A fossil fuel company that operates in the Russian Federation, except if the fossil fuel company transports oil or gas—

(i) Through the Russian Federation for sale outside of the Russian Federation; and
(ii) That was extracted from a country other than the Russian Federation with respect to the energy sector of which the President has not imposed sanctions as of the date on which the contract is awarded.

(End of provision)

The following provisions and clauses are incorporated by reference:

52.203-11 Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions (SEP 2024) FAR DEVIATION 2026-O0038
252.203-7005 Representation Relating to Compensation of Former DoD Officials (SEP 2022) DFARS DEVIATION 2026-O0031
252.204-7008 Compliance with Safeguarding Covered Defense Information Controls (OCT 2016) DFARS DEVIATION 2026-O0025 Revision 2
252.219-7000 Advancing Small Business Growth (JUN 2023) DFARS DEVIATION 2026-O0037

52.222-19 Child Labor—Cooperation with Authorities and Remedies (FEB 2026) FAR DEVIATION 2026-O0038
252.225-7031 Secondary Arab Boycott of Israel (JUN 2005) DFARS DEVIATION 2026-O0041 Revision 1
252.225-7055 Representation Regarding Business Operations with the Maduro Regime (MAY 2022) DFARS DEVIATION 2026-O0041 Revision 1
252.225-7059 Prohibition on Certain Procurements from the Xinjiang Uyghur Autonomous Region–Representation (JUN 2023) DFARS DEVIATION 2026-O0041 Revision 1
252.225-7963, Antiterrorism/Force Protection Policy for Defense Contractors Outside the United States (FEB 2026) DFARS DEVIATION 2026-O0041 Revision 1
52.240-90 Security Prohibitions and Exclusions Representations and Certifications (FEB 2026) FAR DEVIATION 2026-O0038

Section L – Instructions, Conditions, and Notices to Offerors or Respondents

52.252-1 Solicitation Provisions Incorporated by Reference (FEB 1998) FAR DEVIATION 2026-O0038

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es):

FAR - https://www.acquisition.gov/far-overhaul
DFARS - https://www.acq.osd.mil/dpap/dars/dfars_far_overhaul_class_deviations.html unless noted with DFARS, then https://www.ecfr.gov/current/title-48/chapter-2
VAAR - https://www.va.gov/oal/library/vaar/vaar852.asp

(End of Provision)

52.252-5 Authorized Deviations in Provisions (NOV 2020) FAR DEVIATION 2026-O0038

(a) The use in this solicitation of any Federal Acquisition Regulation (48 CFR chapter 1) provision with an authorized deviation is indicated by the addition of (DEVIATION) after the date of the provision.
(b) The use in this solicitation of any Defense Federal Acquisition Regulation Supplement (48 CFR chapter 2) provision with an authorized deviation is indicated by the addition of (DEVIATION) after the name of the regulation.

(End of Provision)

52.212-1 Instructions to Offerors – Commercial Products and Commercial Services (FEB 2026) FAR DEVIATION 2026-O0038 is incorporated in this solicitation by reference.

The following paragraphs of 52.212-1 are amended as indicated:

1. Paragraph (a) - *Submission of Offers*. Delete and replace with the following:

Submission of Offers. This solicitation is a "standing solicitation" which will be open through the date and local time in Block 8 of SF 1449 (Page 3). An offer will be evaluated after submission with Government review prioritized as follows:

Priority 1) A proposal submitted by a firm that has a current contract that is due to expire.

Priority 2) Priority items for award determined by the Government (For example, items that support contingency, introduction of new items, or urgent customer requirements).
Priority 3) All other offers.

Offerors shall use PIEE as directed in Block 9 of SF 1449 to submit their offer. No other method of response is permitted.

The Government shall not be liable for any costs incurred by the offeror in preparation or submission of their proposal.

Unless eligible for Streamlined Offering (described below), offerors shall submit all the following with their offer:

(1) A completed solicitation document with a handwritten or digital signature on the SF 1449. There are fill-ins throughout the solicitation document that require completion.

(2) A completed Attachment A – Vendor Price Book, Attachment B - Discount & Pricing Information (and requested supporting documentation), and Attachment D – Statement of Work Responses per the Attachment Instructions that follow below.

The vendor shall provide other than cost or pricing data in the form of a random sample of commercial invoices, GPO pricing, or other independent data to support the reasonableness of the offered items. The Government reserves the right to require other pricing information or use other price support/sampling procedures than those noted below to ensure that all prices are fair and reasonable.

Commercial Invoices and GPO Sample Instructions:

Offerors are required to submit commercial invoices and/or Group Purchasing Organization (GPO) agreement(s) with their initial proposal. The invoices and/or GPO must be un-redacted. The contractor shall utilize the MACORR Sample Size Calculator (http://www.macorr.com/sample-size-calculator.htm), using a Confidence Level of 90% and a Confidence Interval of 10% for their entire population of items to determine the number of items required to be reviewed. The required sample of items submitted must be of different items, not instances of selling the same item.

In order to support the price reasonableness of the proposed items, the vendor shall complete Attachment #A price support fields (columns S-AA) with the following elements for review, and provide the actual un-redacted invoices and/or GPO data:

(i.) A minimum submission of invoices shall be calculated using the MACORR website listed above. The vendor shall provide the most recent un-redacted commercial invoices or GPO pricing for Most Similar Customer (MSC). The MSC is defined as the most favored customer within a similar purchasing environment as DLA. Customers within a similar purchasing environment should be considered customers of equal size to DLA, with no guaranteed commitment level.

The methodology below should be used to determine the items for which price support information is required based on a vendor's initial price book offer.

1. Sort the initial offer (Attachment #1 spreadsheet) by List Price.

2. Sample should be submitted as follows:
a. 50% of sample size should be highest priced items
b. 25% of sample size should be middle priced items [Starting with median (middle item) and take all higher priced items to cover 25% of sample size]
c. 25% of sample size should be lowest priced items

Note 1: If the above methodology requires price support information for an item that has not been sold or quoted to date, the vendor is required to provide price support information for the next item that has price support information. The vendor must note in column AA and certify that an item has not been sold in their submission.

(ii.) A minimum submission of GPO data or three most recent un-redacted commercial invoices for full systems for the vendor's Absolute Best Priced Customer (ABPC). The ABPC is the customer that currently receives or has received the best pricing (within the past 12 months).

(iii.). If different from the ABPC, a minimum submission of GPO data or three most recent un-redacted commercial invoices for full systems for the vendor's Best Committed Customer. This customer has the highest commitment level to the vendor.

(iv.) A minimum of GPO data or three most recent un-redacted commercial invoices for full systems for the vendor's Best Uncommitted Customer. This customer receives the best pricing when compared to all customers that have no commitment level to the vendor.

(v.) A minimum of three most recent un-redacted commercial invoices for full systems for the vendor's Highest Priced Customer. This customer receives the highest pricing.

(vi.) A single invoice should not be used to cover more than one item with the exception of item (iii.) above.

(vii.) The invoices required for (ii.) through (v.) above should reflect sales within the last 12 months.

(3.) Commercial Price List: Offeror shall submit their current, dated, published commercial price list of all items and maintenance offered in the proposal. This includes price list catalogs or other documentation setting forth the prices charged the general public.

(4) If applicable, a completed Attachment C – Offeror Exceptions to Terms and Conditions, per the Attachment Instructions that follow below.

(5) If the offeror is not a small business for NAICS 334510, a Small Business Subcontracting Plan as set forth in clause 52.219-9.

(6) The company's restocking charge policy, if any, to include restocking charge if any. Restocking fees are not acceptable unless the vendor submits a rationale for these charges that substantiates them as fair and reasonable as determined by the Contracting Officer.

(7) Factor 1 - Product and Maintenance Offering. The Offeror shall provide the following for each Specialty included in the offer:

(A) Provide a comprehensive description and supporting documentation of your proposed PACS product line(s), including key features, all target markets, and technical specifications, clearly identifying the applicable specialization (e.g., Radiology, Cardiology, etc.). Specifications shall detail the functionalities, architecture, and minimum required hardware.
(B) Commercial catalog(s) and Federal Supply Schedule Contracts for the offered products.
(C) Certifications and regulatory approvals relevant to your solution, including proof of FDA 510(k) premarket notification, for all offered products that require this certification.
(D) Attachments A and D will also be used to evaluate the Product Offering factor.

(8) Factor 2 – Past Performance. Provide a description of three distinct installations of your proposed PACS solution within an enterprise-distributed architecture within the last two years. Include:

(A) Customer name and type (e.g. Government or Commercial);

(B) Facility name and type;
(C) Summary of the installation (including a description of integration of the PACS with the existing customer RIS and EHR and study and user volume), estimated cost, and installation timeline; and
(D) Customer contact person and telephone number.
The Government will review any vendor provided information and contact any cited commercial customers to evaluate performance.

(9) Factor 3 - Experience. The Offeror shall provide a written narrative that addresses the following:

(A) The organizational structure of the company including key departments and number of employees within those departments;
(B) The experience of company executives and key personnel, particularly with respect to their professional management and PACS project experience including experience integrating PACS solution(s) with existing government and commercial Radiology Information Systems (RIS) and Electronic Health Records (EHR);
(C) Briefly describe any relevant integration capabilities; and
(D) A description of third-party vendors or business partners whose products or services are integrated into proposed PACS solution(s).

Any other supporting documentation, including invoices not specifically requested by the attachments, are not to be submitted with the initial offer. Additional documentation and invoices will be requested by the Contracting Officer as part of clarifications or negotiations.

Offers found to be missing required information may be rejected without further evaluation.

Streamlined Offering: An offeror that has a current contract under SPE2D1-15-R-0004 (DIN-PACS IV) at the time of submitting an offer on this solicitation is not required to provide information for Paragraph (8) Factor 2 – Past Performance or Paragraph (9) Factor 3 – Experience, provided the offeror:

(1) Is offering under the same Unique Entity Identifier as shown on the SPE2D1-15-R-0004 contract;
(2) Had performance on at least three active delivery orders under the contract SPE2D1-15-R-0004 within two years of submitting an offer on this Solicitation; and
(3) Received CPARS ratings of Satisfactory or better for each category rated on the SPE2D1-15-R-0004 contract for completed CPARS within two years of submitting an offer on this Solicitation.

For streamlined offers, the Government will evaluate the offeror's Past Performance and Experience according to 52.212-2 using internal information but reserves the right to request additional information related to the offeror's Experience and Past Performance after offer submission.

Attachment Instructions:

(1) Attachment A – Vendor Price Book.

1. The Vendor Price Book is included in the official contract schedule and must include all part numbers, item descriptions, vendor list prices, contract discounts, and other required information. All proposed contract offerings and pricing must be submitted using Attachment A. Complete the Vendor Price Book according to the Instructions Tab within the Excel workbook and column instructions on the other Tab. The format shall not be altered in any way (e.g. no macros, embedded formulas, new columns, new tabs). Some protections are included in Attachment A to prevent alterations. Only one Attachment A is permitted, with the following authorized tabs:
- Instructions
- Vendor Info
- Product Offering
- Maintenance Offering
- Product XLOOKUP
- Maintenance XLOOKUP

If a vendor finds Attachment A does not function correctly for any reason, they should contact the Government Points of Contact listed in this Solicitation.

Offerors are encouraged to submit multiple commercial products that satisfy the requirements of this solicitation. All items offered shall be listed in Attachment A – Vendor Price Book.

(2) Attachment B – Price and Discount Information. Complete the two tabs PRICING INFO and DISCOUNTING INFO according to the instructions provided on the INSTRUCTIONS tab within the attachment. Supporting information submitted pursuant to the instructions shall be clearly marked as support for Attachment B in the offeror's proposal.

(3) Attachment C – Offeror Exceptions to Terms and Conditions (Reference Caution Notice 3). Except for exceptions to the Statement of Work, the Offeror shall use Attachment C to list all offeror exceptions to provisions and clauses in the solicitation, or any terms and conditions. Each exception shall include:

(A) a reference to the solicitation page number, attachment page number, etc.;
(B) the specific provision, clause, paragraph, or requirement, that exception is taken to; and
(C) a clear statement of the exception and the reasons for the exception.

(4) Attachment D – Statement of Work Responses. This spreadsheet has a tab for each specialty in the Statement of Work and Appendix 1. The rows for each tab correspond to a numbered paragraph in the Statement of Work. For each specialty offered and for each Appendix, the Offeror shall complete Column C with a statement of how their product offering meets the requirement and a reference to any documentation provided that supports the statement. The Offeror shall also complete the Specialty Matrix tab, where the Offeror shall indicate which specialties are offered on the contract. The Offeror-completed matrix will be used to determine which contractors shall be considered for fair opportunity orders, provided the Offeror's products meet the requirements in the Statement of Work.

(5) Attachment E – Modification Check List, and Attachment F – Modification Spreadsheet are included for reference. Attachments F and G shall be used for Modification requests during any resultant contract.

(6) Attachment G – VA Handbook 6500.6 Appendix A - Checklist for Information Security in the Initiation Phase of Acquisitions and Attachment H – VA Directive 6550 Appendix A pertain to VA delivery orders.

2. **Paragraph (b) -** *Period for Acceptance of Offers.*

Change "30 calendar days" to read "**240**" calendar days."

4. **Paragraph (d) -** *Contract Award.* Add the following after the last sentence: The Government plans to award multiple contracts under FAR 16.504 for the same or similar supplies under this solicitation, and order pursuant to FAR 16.506 and 16.507.

(End 52.212-1)

The following additional instructions apply:

1) Contract Term. The anticipated term of contracts will be: (1) a five-year base period and one five-year option period for awards made within five years of solicitation issuance, or (2) a single five-year period for awards made after five years of solicitation issuance.

2) Contract Maximum. A contract maximum shall be established by the Government for each individual contract through analysis of available information that may include analysis of previous sales, commercial sales, or other methods. This single maximum contract limitation shall apply for life of the contract, including the base term and any option term, if exercised. All vendors with estimated annual sales under the Program of $10 million or greater

may be subject to a commercial pricing audit conducted by the VA Office of Inspector General. The Government reserves the right to invoke audits at any time.

3) Guaranteed Minimum. The guaranteed minimum for each basic contract is $3,000. The guaranteed minimum for an exercised option term is also $3,000. The Government may fulfill each guarantee by a single delivery order or by any number of delivery orders.

4) Pricing Support for Price Reasonableness Determinations: For initial contract award and any contract modification the vendor shall provide other than certified cost or pricing data to support the price reasonableness of the offered items or changes, as requested by the Contracting Officer. See DFARS 252.215-7994 and FAR 52.215-21 included in this solicitation. Notwithstanding the inclusion of any item on the contract, the Contracting Officer may remove that item if its price is later found not to be fair and reasonable or found to be out of the contract's scope.

(A) As part of clarifications or negotiations, the offeror will be required to submit invoices and/or other documentation to substantiate commercial catalog prices and discounts for offered items. This data will also be used to substantiate that prices offered are equal to or better prices that are given to the commercial customers within similar purchasing environments. A similar purchasing environment consists of customers that purchase under the same constraints as the Federal Government, the combination of all DLA and VA orders, with no guaranteed commitment level.

b) At the discretion of the Contracting Officer a random sampling technique may be used to limit the number of items for which a vendor has to provide price support information, both for items in initial offers and for product additions after contract award. The vendor will be provided direction on which items require price support information as part of clarifications prior to initial contract award, or when vendors submit product modification requests after contract award. Invoices shall be the most recent commercial invoice reflecting the same list price as item(s) to be added. If a vendor does not have any invoices, then the vendor can provide current or the most recent commercial quotes.

If using quotes, the vendor must also supply the accompanying purchase order reflecting that the vendor's customer accepted the quote amount. The Government may request invoices for these items later. This may be through an audit later either as part of option exercise (in addition to normal sample population for option review) or as a separate audit. If the item is completely new and has not yet been quoted, the vendor can use a similar item and provide information outlining differences/similarities between the items that justify the offered price.

The Government reserves the right to require other pricing information or use other price support procedures during the life of the contract to ensure that all prices are fair and reasonable. Failure to provide adequate supporting information for the Contracting Officer to determine pricing as fair and reasonable shall result in rejection of the offer or addition request.

Other than certified cost or pricing data can be a mix of invoices, quotes with Purchase Orders (Pos), and similar items already on contract. Do not submit invoices or quotes that are under different buying circumstances such as volume buys or committed customer discounts. These are unusable and do not count toward satisfying the sample size as the Government can only review invoices for customers buying under the same conditions as the Government. Invoices and quotes must clearly indicate the list price of the items as well as net price.

Invoices must be current (dated within the last 12 months); however, the contracting officer may consider older dated invoices if necessary. Invoice list prices must MATCH offered list prices of added items for review.

5) Price Reasonableness Determinations for items not pre-priced under contract: Under certain circumstances vendors are unable to set a fixed price for items such as incidental/professional services or third-party items at time of basic contract award. For such items vendor must provide their methodology for establishing their price for such items. This method must be the same as offered commercially. This method will be used to add these

items to the contract. . For delivery orders that contain the items that could not be pre-priced at time of award, the price must be determined to be fair and reasonable by the Contracting Officer prior to any order being issued. Upon request, the vendor shall be required to provide price support to the Government to assist in determining the proposed pricing as being fair and reasonable. The price support should validate the methodology that was established at the time the item was added to contract. This may include, but not be limited to other than certified cost or pricing data, commercial invoices for same or similar incidental service, subcontractor quotes for exact work, third-party manufacturer quotes, etc.

6) Questions: Prospective offerors are encouraged to review the solicitation in its entirety and submit any questions or requests for clarification in writing to Christine.Welker@dla.mil and Zahkiyah.Taylor@dla.mil. All questions must be received no later than April 14, 2033 at 3:00pm Eastern Time. Questions submitted after this deadline may not be considered. Questions shall identify the solicitation number and reference the applicable section, attachment, or requirement. The Government will review questions received and, as appropriate, publish a consolidated Questions and Answers (Q&A) document on Procurement Integrated Enterprise Environment (PIEE) at https://piee.eb.mil/ for the benefit of all prospective offerors. Questions may be edited to remove identifying or proprietary information prior to publication. Offerors are responsible for monitoring PIEE for any updates, clarifications, or amendments to the solicitation. Only a formal written solicitation amendment issued by the Contracting Officer may modify the requirements, terms, or conditions of this solicitation.

(End of Additional Instructions)

52.216-1 – Type of Contract (FEB 2026) FAR DEVIATION 2026-O0038

The Government contemplates award of a **FIXED PRICE WITH ECONOMIC PRICE ADJUSTMENT, INDEFINITE –DELIVERY, INDEFINITE QUANTITY** contract resulting from this solicitation.

(End of provision)

L02 Electronic Order Transmission (JUN 2020) DLAD

Offerors shall select one of the following alternatives for paperless order transmission:

[ ] American National Standards Institute (ANSI) X12 Standards through a value added network (VAN) approved by DLA Transaction Services; or
[ ] Electronic mail (email) award notifications containing web links to electronic copies of the Department of Defense (DD) Form 1155, Order for Supplies or Services. Offerors must register on the DLA Internet Bid Board System (DIBBS) (https://www.dibbs.bsm.dla.mil/) to receive email notification. If the offeror elects ANSI/VAN order transmission, DLA will send Electronic Data Interchange (EDI) transaction sets at time of award. The contractor shall acknowledge receipt of transaction sets with a functional acknowledgement or order receipt message within 24 hours. If the contractor receives the award transaction set on a weekend or Federal holiday, the contractor shall acknowledge receipt on the next business day. This acknowledgement will confirm that the contractor's interface with the system is working as needed for contract ordering. Offerors can obtain information regarding EDI, ANSI X12 transactions, and VANs approved by DLA Transaction Services at Defense Automatic Addressing System (DAAS) Value Added Network List (https://www.transactionservices.dla.mil/daashome/edi-vanlist-dla.asp). Offerors should direct questions concerning electronic ordering to the appropriate procuring organization point of contact below: DLA Land and Maritime, Helpdesk.EBS.L&M.LTCs@dla.mil DLA Troop Support, dlaedigroup@dla.mil DLA Aviation, avnprocsysproceddiv@dla.mil, phone # 804-279-4026 *****

L06 Agency Protests (DEC 2016) DLAD

Interested parties may file an agency level protest with the contracting officer or may request an independent review by the chief of the contracting office (CCO). Independent review by the CCO is an alternative to consideration by the contracting officer and is not available as an appellate review of a contracting officer decision on a protest previously

filed with the contracting officer. Absent a clear indication of the intent to file an agency level protest with the CCO for independent review, protests will be presumed to be protests to the contracting officer.

(End of Provision)

L29 Section 508 Requirements (OCT 2021) DLAD

Offerors shall comply with the Section 508 accessibility requirements. By submission of its offer, the offeror affirms that its Information and Communication Technology (ICT) supplies and services are accessible as outlined in the law, the standard, and FAR Subpart 39.2. Offerors shall complete the current revision of the Voluntary Product Accessible Template (VPAT) Rev 508 at https://www.itic.org/policy/accessibility/vpat (copy website address into browser). If applicable, offerors shall indicate where their Section 508 ICT compliance information is available for review (e.g., offeror's website or other location the contracting officer can access). The contracting officer may require a demonstration of Section 508 compliance prior to award.

(End of Provision)

L31 Additive Manufacturing (JUN 2018) DLAD

(1) Additive manufacturing (AM) is a process of joining materials to make objects from three-dimensional (3D) model data, usually layer upon layer, as opposed to subtractive manufacturing methodologies, which remove material from areas where it is not desired, or other traditional manufacturing technologies, such as molding or stamping.

(2) Unless AM is specifically authorized in the solicitation/contract, offers may not include parts or supplies made using the additive manufacturing process. The Government will not evaluate offers that include an item or items produced using AM, and such quotes/offers are not eligible for award for the current procurement. A quoter/offeror proposing to supply an AM-produced item may submit a request to the contracting officer for approval of the item for evaluation by the Engineering Support Activity (ESA) for acceptability for future procurements of the same items.

(3) If an item produced using AM is presented to the Government for inspection and acceptance that was not authorized in the solicitation/contract, the Government may reject the item as nonconforming.

(End of Clause)

5452.233-9001 Disputes - Agreement to Use Alternative Dispute Resolution (ADR) (JUN 2020) DLAD

(a) The parties agree to negotiate with each other to try to resolve any disputes that may arise. If unassisted negotiations are unsuccessful, the parties will use alternative dispute resolution (ADR) techniques to try to resolve the dispute. Litigation will only be considered as a last resort when ADR is unsuccessful or has been documented by the party rejecting ADR to be inappropriate for resolving the dispute.
(b) Before either party determines ADR inappropriate, that party must discuss the use of ADR with the other party. The documentation rejecting ADR must be signed by an official authorized to bind the contractor (see FAR 52.233-1), or, for the Agency, by the contracting officer, and approved at a level above the contracting officer after consultation with the ADR Specialist and legal counsel. Contractor personnel are also encouraged to include the ADR Specialist in their discussions with the contracting officer before determining ADR to be inappropriate.
(c) If you wish to opt out of this clause, check here **[ ]**. Alternate wording may be negotiated with the contracting officer.

(End of Provision)

Additional provisions incorporated by reference:

52.203-18 Prohibition on Contracting with Entities that Require Certain Internal Confidentiality Agreements or Statements—Representation (JAN 2017) FAR DEVIATION 2026-O0038

52.204-7 System for Award Management-Registration (FEB 2026) FAR DEVIATION 2026-O0038
252.215-7994 Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data (MAR 2026) DFARS DEVIATION 2026-O0048
52.216-27 Single or Multiple Awards (OCT 1995) FAR DEVIATION 2026-O0038
52.222-56 Certification Regarding Trafficking in Persons Compliance Plan (FEB 2026) FAR DEVIATION 2026-O0038
52.233-2 Service of Protest (FEB 2026) FAR DEVIATION 2026-O0038
252.246-7006 Warranty Tracking of Serialized Items (MAR 2016) DFARS DEVIATION 2026-O0035
252.239-7017 Notice of Supply Chain Risk (DEC 2022) DFARS DEVIATION 2026-O0025 Revision 2

Section M – Evaluation Factors for Award

52.212-2 Evaluation – Commercial Products and Commercial Services (FEB 2026) RFO DEVIATION 2026-O0038

(a) The Government intends to award a contract to all responsible offerors whose offers conforming to the solicitation will be advantageous to the Government, price and other factors considered.

Technical (non-price). The following non-price factors shall be used to evaluate offers and determine technical acceptability:

(1) Product and Maintenance Offering
(2) Past Performance
(3) Experience

Factors (1) through (3) will be evaluated on an acceptable/unacceptable basis. In conducting the evaluation, the Contracting Officer will use information provided by the offeror in its proposal. The burden is on the offeror to provide a complete and thorough proposal. Missing proposal information or component(s) identified above and/or non-adherence to proposal format instructions provided in provision 52.212-1 of the solicitation will be considered incomplete. As a result, the offeror may be eliminated from further consideration of award.

(1) Product and Maintenance Offering

Acceptable: Proposal meets the requirements of the solicitation.

Unacceptable: Proposal does not meet the requirements of the solicitation.

(2) Past Performance

Acceptable: Based on the offeror's performance record, the Government has a reasonable expectation that the offeror will successfully perform the required effort, or the offeror's performance record is Unknown. A performance record will be determined Unknown if the offeror's record regarding PACS installations within an enterprise-distributed architecture for the two years prior to offer submission is so sparse that no meaningful confidence assessment rating can be reasonably assigned.

Unacceptable: Based on the offeror's performance record, the Government does not have a reasonable expectation that the offeror will be able to successfully perform the required effort.

(3) Experience

Acceptable: Based on the offeror's experience, the Government has a reasonable expectation that the offeror will successfully perform the required effort.

Unacceptable: Based on the offeror's experience, the Government does not have a reasonable expectation that the offeror will be able to successfully perform the required effort.

Experience will only be evaluated when an Offeror receives a Past Performance rating of Acceptable by virtue of having an Unknown performance record.

Overall Technical Evaluation. The offeror must have an Acceptable rating in each rated factor to receive an overall Acceptable rating. Only those offers determined to be overall technically acceptable will be considered for award.

Price: All offered pricing must be determined to be fair and reasonable for an offeror to be considered for award. Other than certified cost or pricing data will be provided and evaluated to ensure that offered pricing is equal to or better than pricing that the vendor offers to their most favored customers under a similar contracting environment. A VA OIG price audit may be conducted for those vendors with estimated annual sales over $10 million.

Award: Only those offerors who are found to be Acceptable under the Overall Technical Evaluation and have fair and reasonable pricing shall receive an award.

(b) *Options*. There will be no option pricing in the offer. Any changes to pricing will be governed by the Economic Price Adjustment clause.

(c) *Notice of award.* A written notice of award or acceptance of an offer furnished to the successful Offeror within the time for acceptance specified in the offer, shall result in a binding contract without further action by either party. Before the offer's specified expiration time, the Government may accept an offer (or part of an offer), whether or not there are negotiations after its receipt, unless a written notice of withdrawal is received before award.

VA Issued Delivery Orders

THE FOLLOWING SECTION PERTAINS
TO VA ISSUED DELIVERY ORDERS ONLY

VA ORDERING PROCEDURES

1. Ordering.

The PACS Delivery Orders will be awarded by the VA NAC or VA Authorized Users to the awarded IDIQ contractors for any contracted PACS item(s), furnished under this contract. All Delivery Orders are subject to the terms and conditions of this contract. In the event of conflict between a Delivery Order and this contract, this contract will be given precedence.

Delivery Orders will include:

- DIN PACS V Contract number including Delivery Order number
- Description of the equipment and/or deliverables to be inspected
- Unit prices and delivery schedules
- Accounting and Appropriation Data
- The Delivery/Installation Location (Hospital/Facility Name, Room # & Base/City/State).

2. Delivery.

- Delivery times and methods will be specified per individual Delivery Order.
- When requested Contractors shall provide appropriate documentation (packing slips and proof of delivery/bill of lading) referencing the Delivery Order deliverables.

3. Invoicing Instructions

Invoice. Electronic invoices shall be used as follows:

Payment Office and Invoicing Instructions for VA Delivery Orders Only:

Contractors shall submit invoices for payment electronically in accordance with VAAR Clause 852.232-72 Electronic Submission of Payment Requests. The contractor shall submit the invoices through the Tungsten e-Invoice Network (https://authentication.tungsten-network.com/login).

TRAINING OF OPERATING PERSONNEL (MAY 1995)

The price quoted shall include contractor responsibility for providing on-site orientation and training of two using personnel in operation and care of the equipment furnished. This training shall include actual demonstration and operation of the equipment including any adjustments or other actions which may be undertaken by operating personnel in the event of failure of equipment, provided that such adjustment or action will in no way jeopardize the Government's rights under contract guarantee clause. This training will be given by qualified contractor personnel upon completion of installation. The contractor will consult with the Authorized Customer POC at the site (or person acting in that capacity) regarding the time this training will begin. That official will be responsible for arranging for the presence of personnel to be trained.

PRODUCT MODIFICATION, REMOVAL OR RECALL (MAR 2005)

If any product awarded under this solicitation requires modification, is removed or recalled by the contractor or manufacturer, or if any required modification, removal or recall is suggested or mandated by a regulatory or official agency, the following steps will immediately be taken by the contractor or manufacturer:

a. Notify the VA Contracting Officer (CO) by email notification which shall include, but not be limited to the following:
   i. Complete item description and/or identification, order numbers from customers, and the contract number assigned as a result of an award on this solicitation.
   ii. Reasons for modifications, removal or recall.
   iii. Necessary instructions for return for credit, replacement or corrective action.
b. Provide the above information to all agencies and VA Facilities who purchased the product.
c. The VA shall be provided a copy of the notification in b. above, and a list of all agencies and/or VA facilities notified.

852.233-70 Protest Content/Alternative Dispute Resolution (SEP 2018) – VA Delivery Orders Only

852.233-71 Alternate Protest Procedure. (SEP 2018) – VA Delivery Orders Only

(a) As an alternative to filing a protest with the Contracting Officer, an interested party may file a protest by mail or electronically with: Executive Director, Office of Acquisition and Logistics, Risk Management and Compliance Service (003A2C), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC20420 or Email: EDProtests@va.gov.

(b) The protest will not be considered if the interested party has a protest on the same or similar issue(s) pending with the Contracting Officer.