AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT

BPA NO.	1. CONTRACT ID CODE	PAGE	OF PAGES
		1	105

2. AMENDMENT/MODIFICATION NUMBER	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQ. NUMBER	5. PROJECT NUMBER (if applicable)
0002			VA-26-00035665

6. ISSUED BY CODE	7. ADMINISTERED BY (If other than Item 6) CODE
Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724	Department of Veterans Affairs Technology Acquisition Center 23 Christopher Way Eatontown NJ 07724

8. NAME AND ADDRESS OF CONTRACTOR (Number, street, county, State and ZIP Code)	(X)	9A. AMENDMENT OF SOLICITATION NUMBER
To all Offerors/Bidders		36C10B26R0039
	X	9B. DATED (SEE ITEM 11) 7/30/2026
	☐	10A. MODIFICATION OF CONTRACT/ORDER NUMBER
		10B. DATED (SEE ITEM 13)
CODE / FACILITY CODE		

11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS

☒ The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offers ☐ is extended, ☒ is not extended.

Offers must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended, by one of the following methods:

(a) By completing Items 8 and 15, and returning _____ copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or electronic communication which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by letter or electronic communication, provided each letter or electronic communication makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.

12. ACCOUNTING AND APPROPRIATION DATA (If required)

13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS, IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.

CHECK ONE	
☐	A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.
☐	B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(b).
☐	C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:
☐	D. OTHER (Specify type of modification and authority)

E. IMPORTANT: Contractor ☐ is not, ☒ is required to sign this document and return 1 copies to the issuing office.

14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.)

See Continuation Page.

Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.

15A. NAME AND TITLE OF SIGNER (Type or print)		16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)	
		Stefanie Applegate Contracting Officer	
15B. CONTRACTOR/OFFEROR (Signature of person authorized to sign)	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA (Signature of Contracting Officer)	16C. DATE SIGNED

CONTINUATION PAGE

The purpose of this amendment (0002) to Request for Quotation (RFQ) 36C10B26R0039 is in red as follows:

1. Provide the Government's response to questions posed by industry. See attached "Attachment 1 – Amendment 0002 QA - DSS Infusion Therapy Manager Solicitation 36C10B26R0039".

2. Update the quantities listed in the Product Description to meet the Government's requirements.

3. Update language in section E.12.(2)(c)(ii)(1) VOLUME II – PAST PERFORMANCE FACTOR to allow vendors to provide Section 1 information in excel and will not Section 1 as a part of the 5 page limitation.

4. All changes to the solicitation based on the aforementioned alterations are incorporated within the attached RFP 36C10B26R0039 Rev 2. Except as described herein, all other terms and conditions remain unchanged.

Table of Contents

SECTION B - CONTINUATION OF SF 1449 BLOCKS 5

B.1 REQUIREMENTS BACKGROUND 5
B.2 SCHEDULE OF SUPPLIES AND SERVICES 5
B.3 CONTRACT ADMINISTRATION DATA 36
B.4 GOVERNING LAW 37
B.5 SOFTWARE LICENSE, MAINTEANCE AND TECHNICAL SUPPORT 38
B.6 ACCOUNTING AND APPROPRIATION DATA 40
B.7 ORDERING PROCEDURES 40
B.8 PRODUCT DESCRIPTION 41

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE 53

SECTION C - CONTRACT CLAUSES 67

C.1 ADDENDUM to RFO 52.212-4 TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES 67
C.2 RFO FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998) 67
C.3 RFO 52.216-18 ORDERING (AUG 2020) 70
C.4 RFO 52.216-19 ORDERING LIMITATIONS (OCT 1995) 70
C.5 RFO 52.216-22 INDEFINITE QUANTITY (NOV 2025) 71
C.6 VAAR 852.204-70 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (MAY 2020) 71
C.7 VAAR 852.204-71 INFORMATION AND INFORMATION SYSTEMS SECURITY (MAR 2026) 71
C.8 852.204-72 PERSONNEL VETTING AND CREDENTIALING (MAR 2026) 80
C.9 852.211-76 LIQUIDATED DAMAGES—REIMBURSEMENT FOR DATA BREACH COSTS (FEB 2023) 83
C.10 VAAR 852.222-71 COMPLIANCE WITH EXECUTIVE ORDER 13899 (APR 2025) (DEVIATION) 84

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS 85

Attachment 1 – Amendment 0002 QA - DSS Infusion Therapy Manager Solicitation 36C10B26R0039 ..... **Error! Bookmark not defined.**

SECTION E - SOLICITATION PROVISIONS 86

E.1 FAR 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998) 86
E.2 RFO 52.203-11 CERTIFICATION AND DISCLOSURE REGARDING PAYMENT TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (SEP 2024) 86
E.3 52.209-12 CERTIFICATION REGARDING TAX MATTERS (OCT 2025) 87
E.4 RFO 52.216-1 TYPE OF CONTRACT (NOV 2025) 87
E.5 RFO 52.219-4 NOTICE OF PRICE EVALUATION PREFERENCE FOR HUBZONE SMALL BUSINESS CONCERNS (DEV NOV 2025) 88
E.6 RFO 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEV NOV 2025) 88

E.7 RFO 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (DEV NOV 2025) 89
E.8 VAAR 852.215-72 NOTICE OF INTENT TO RE-SOLICIT (OCT 2019) 92
E.9 VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (SEP 2018)....92
E.10 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (SEP 2018) 93
E.11 VAAR 852.273-70 LATE OFFERS (NOV 2021) 93
E.12 INSTRUCTIONS TO OFFERORS....93
E.13 BASIS OF AWARD 100

SECTION H - SPECIAL CONTRACT REQUIREMENTS....103

H.1 ARTIFICIAL INTELLIGNENCE IN VA CONTRACTS 103

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 REQUIREMENTS BACKGROUND

This is a solicitation for commercial items prepared in accordance with the format in Revolutionary Federal Acquisition Regulation Overhaul (RFO) Subpart 12.6, as supplemented with additional information included in this notice. Request for Proposal (RFP) 36C10B26R0039 is issued to fulfil The Department of Veterans Affairs requirement for Document Storage Systems (DSS) Infusion Therapy Manager (ITM) licenses software and ancillary services to include maintenance, delivery, installation, testing, implementation, and training. The resulting contract, if any, will be an Indefinite-Delivery/ Indefinite-Quantity (IDIQ) type contract, as described in RFO 16.504, with Delivery Orders (DO) placed against the contract to order and fund individual requirements. This action is solicited as unrestricted, under North American Industrial Classification System (NAICS) Code 513210 “Software Publishers.” The size standard for NAICS 513210 is $47M. Specific requirements are listed in the “Product Description” (see section B.9). All proposals shall contain the minimum information required under RFO Clause 52.212-1 Instructions to Offerors-Commercial Products and Commercial Services, to include its associated addendum (see section E.12). All proposals received in response to this solicitation will be evaluated in accordance with section E.13 BASIS OF AWARD. All questions should be sent to John Sangalang at john.sangalang@va.gov by 3:00PM Eastern Daylight Time on July 29, 2026.

The IDIQ total ordering period is five years beginning day of award through five years after award (specific dates to be provided at award). IAW RFO 52.216-19 the minimum guaranteed amount under the national DSS ITM IDIQ contract is $1,200,000.00.

The Government reserves the right to award initial orders at the time of the basic contract award at amounts which may exceed the minimum guaranteed value.

System updates may lag policy updates. The System for Award Management (SAM) may continue to require entities to complete representations based on provisions that are not included in agency solicitations. Contracting officers rely on representations from offers based on provisions in the solicitation. Entities are not required to, nor are they able to, update their entity registration to remove these representations in SAM.

B.2 SCHEDULE OF SUPPLIES AND SERVICES

NOTE: Vendors are instructed to complete section B.2 Price Schedule and submit with their proposal. Vendors are cautioned that alterations to the line items as specified below may render proposals unacceptable for award.

Any resulting contract will be awarded on a Firm-Fixed-Price basis as defined by RFO Subparts 16.202 and 16.601. Accordingly, the Contractor shall ensure that any and all costs associated with the Contractor’s proposed application(s), software products, software solution, and/or system, shall be included in the Contractor’s proposed firm-fixed price portion of this contract, and shall serve as the Contractor’s firm-fixed price portion for the life of any resulting contract. No additional costs or fees relative to the Contractor’s proposed application(s), software products, software solution, and/or system including, but not limited to, licensing costs and any associated licensing maintenance required for the development, delivery, integration, operation, and/or

maintenance of the Contractor's proposed solution will be allowed, accepted, and/or paid by the Government. Software shall be delivered within five business day of award.

Ordering Periods (Five 12-month Ordering Periods with exact dates to be determined and specified at award):

Ordering Period 1: 12 months from award
Ordering Period 2: 12 months from completion of Ordering Period 1
Ordering Period 3: 12 months from completion of Ordering Period 2
Ordering Period 4: 12 months from completion of Ordering Period 3
Ordering Period 5: 12 months from completion of Ordering Period 4

All deliverables must be submitted to the VA Program Manager (PM), Contracting Officer's Representative (COR), and Contracting Officer (CO) unless otherwise specified in the line item. Please be advised that in accordance with RFO Part 2.101, a "day" means, unless otherwise specified, a Calendar Day. Additionally, deliverables with due dates falling on a weekend or holiday shall be submitted the following Government workday after the weekend or holiday.

The Contracting Officer is authorized to issue task orders via electronic commerce methods.

	Ordering Period 1: **The Period of Performance shall be from day of award through 365 days after award. (Actual dates to be provided at award)**				
Line Item	**Description**	**Max QTY**	**Unit**	**Unit Price**	**Extended Price**
Products					
0001	Firm Fixed Price (FFP) DSS ITM Annual Limited License, Level 1 Facility. DSS-ITM-VA-LL-LVL1 IAW Product Description (PD) Section 1.3 Product Service Code (PSC): DA10 Schedule and delivery to be determined at the order level.	50	Each (EA)	$	$
0002	FFP DSS ITM Annual Limited License, Level 2 Facility. DSS-ITM-VA-LL-LVL2 IAW PD Section 1.3	5	EA	$	$

	PSC: DA10 Schedule and delivery to be determined at the order level.				
0003	FFP DSS ITM Annual Limited License, Level 3 Facility. DSS-ITM-VA-LL-LVL3 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	7	EA	$	$
0004	FFP DSS ITM Analytics Annual Limited License, per facility. DSS-ITM-Analytics-VA-LL IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	62	EA	$	$
0005	FFP DSS VistA Chemotherapy Manager Large Hospital Annual Limited License. DSS-VCM-LTD-LH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	5	EA	$	$
0006	FFP DSS VistA Chemotherapy Manager Medium Hospital Annual Limited License. DSS-VCM-LTD-MH IAW PD Section 1.3 PSC: DA10	1	EA	$	$

	Schedule and delivery to be determined at the order level.				
0007	FFP DSS VistA Chemotherapy Manager Small Hospital Annual Limited License. DSS-VCM-LTD-SH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	1	EA	$	$
Services					
0008	FFP DSS Remote Installation Services Per Day. DSS-INST-R IAW PD Section 1.4 PSC: DA10	62	EA	$	$
0009	FFP EMR Technical Installation Services Per Hour. EMRTEC IAW PD Section 1.4 PSC: DA10	500	Hours (HR)	$	$
0010	FFP DSS Project Management, for new installations, price per hour. PROJ-MGMNT IAW PD Section 1.4 PSC: DD01	2750	HR	$	$
0011	FFP EMR Training Per Hour. EMRTRN IAW PD Section 1.4 PSC: U009	15400	HR	$	$
0012	FFP DSS ADHOC Premium Application Workflow Support - Remote, per facility annual fee. DSS-PREMAPPSUPPORT-VAAF	62	EA	$	$

	IAW PD Section 1.4 PSC: DA10				
0013	FFP Travel Expenses Per Person Per Week TRAVEL-Z IAW PD Section 1.4 PSC: V999	750	EA	$	$
0014	FFP DSS Project Management, is for existing installations, Training and Analysis On-Site or Remote. DSS-PROD-SVC IAW PD Section 1.4 PSC: U099	160	HR	$	$
0015	FFP Conversion of DSS VistA Chemotherapy Manager (VCM) customers to DSS Infusion Therapy Manager (ITM). DSS-ITM-VA Conversion IAW PD Section 1.4 PSC: DA10	14	EA	$	$
0016	FFP DSS VistA Chemotherapy Manager (VCM) Large Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-LH-M IAW PD Section 1.4 PSC: DA10	5	EA	$	$
0017	FFP DSS VistA Chemotherapy Manager Medium Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-MH-M IAW PD Section 1.4	1	EA	$	$

	PSC: DA10				
0018	FFP DSS VistA Chemotherapy Manager Small Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-SH-M IAW PD Section 1.4 PSC: DA10	1	EA	$	$
0019	Deliverable A: Training Plan and Related Documentation IAW PD Section 1.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	Lot (LT)	Not Separately Priced (NSP)	NSP
0020	Deliverable A: Master Delivery Schedule IAW PD Section 4.0. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
0021	Deliverable B: Kick-off Meeting Agenda IAW PD Section 4.0 PSC: DD01 Deliverable due within 10 days of task order award.	1	LT	NSP	NSP
0022	Deliverable C: Shipment/Delivery Weekly Progress Report IAW PD Section 4.0.	52	EA	NSP	NSP

	PSC: DD01 Delivery due on a weekly basis upon task order award through close out.				
0023	Deliverable A: Statement of Attestation IAW PD Section 5.7. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
0024	Deliverable A: Compliance Monitoring and Reporting Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
0025	Deliverable B: Corrective Action Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
0026	Deliverable A: AI Model/LLM Change Disclosure IAW PD Section 5.7.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP

0027	Deliverable A: Contractor Staff Roster IAW PD Section 6.2.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
	Total Ordering Period 1			**$**	

	Ordering Period 2: **The Period of Performance shall be from completion of Ordering Period 1 through 366 days after completion of Ordering Period 1. (Actual dates to be provided at award)**				
Line Item	**Description**	**Max QTY**	**Unit**	**Unit Price**	**Extended Price**
	Products				
1001	Firm Fixed Price (FFP) DSS ITM Annual Limited License, Level 1 Facility. DSS-ITM-VA-LL-LVL1 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	65	EA	$	$
1002	FFP DSS ITM Annual Limited License, Level 2 Facility. DSS-ITM-VA-LL-LVL2 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	4	EA	$	$
1003	FFP DSS ITM Annual Limited License, Level 3	6	EA	$	$

	Facility. DSS-ITM-VA-LL-LVL3 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.				
1004	FFP DSS ITM Analytics Annual Limited License, per facility. DSS-ITM-Analytics-VA-LL IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	75	EA	$	$
1005	FFP DSS VistA Chemotherapy Manager Large Hospital Annual Limited License. DSS-VCM-LTD-LH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	5	EA	$	$
1006	FFP DSS VistA Chemotherapy Manager Medium Hospital Annual Limited License. DSS-VCM-LTD-MH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	1	EA	$	$
1007	FFP DSS VistA Chemotherapy Manager Small Hospital Annual	1	EA	$	$

	Limited License. DSS-VCM-LTD-SH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.				
Services					
1008	FFP DSS Remote Installation Services Per Day. DSS-INST-R IAW PD Section 1.4 PSC: DA10	10	EA	$	$
1009	FFP EMR Technical Installation Services Per Hour. EMRTEC IAW PD Section 1.4 PSC: DA10	80	HR	$	$
1010	FFP DSS Project Management, for new installations, price per hour. PROJ-MGMNT IAW PD Section 1.4 PSC: DD01	450	HR	$	$
1011	FFP EMR Training Per Hour. EMRTRN IAW PD Section 1.4 PSC: U009	2480	HR	$	$
1012	FFP DSS ADHOC Premium Application Workflow Support - Remote, per facility annual fee. DSS-PREMAPPSUPPORT-VAAF IAW PD Section 1.4 PSC: DA10	75	HR	$	$
1013	FFP Travel Expenses Per Person Per Week	200	EA	$	$

	TRAVEL-Z IAW PD Section 1.4 PSC: V999				
1014	FFP DSS Project Management, is for existing installations, Training and Analysis On-Site or Remote. DSS-PROD-SVC IAW PD Section 1.4 PSC: U099	1900	HR	$	$
1015	FFP Conversion of DSS VistA Chemotherapy Manager (VCM) customers to DSS Infusion Therapy Manager (ITM). DSS-ITM-VA Conversion IAW PD Section 1.4 PSC: DA10	2	EA	$	$
1016	FFP DSS VistA Chemotherapy Manager (VCM) Large Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-LH-M IAW PD Section 1.4 PSC: DA10	5	EA	$	$
1017	FFP DSS VistA Chemotherapy Manager Medium Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-MH-M IAW PD Section 1.4 PSC: DA10	1	EA	$	$
1018	FFP DSS VistA Chemotherapy Manager Small Hospital Software Subscription Maintenance	1	EA	$	$

	and Support. DSS-VCM-PERP-SH-M IAW PD Section 1.4 PSC: DA10				
1019	Deliverable A: Training Plan and Related Documentation IAW PD Section 1.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
1020	Deliverable A: Master Delivery Schedule IAW PD Section 4.0. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
1021	Deliverable B: Kick-off Meeting Agenda IAW PD Section 4.0 PSC: DD01 Deliverable due within 10 days of task order award.	1	LT	NSP	NSP
1022	Deliverable C: Shipment/Delivery Weekly Progress Report IAW PD Section 4.0. PSC: DD01 Delivery due on a weekly basis upon task order award through close out.	1	EA	NSP	NSP

1023	Deliverable A: Statement of Attestation IAW PD Section 5.7. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
1024	Deliverable A: Compliance Monitoring and Reporting Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
1025	Deliverable B: Corrective Action Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
1026	Deliverable A: AI Model/LLM Change Disclosure IAW PD Section 5.7.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
1027	Deliverable A: Contractor Staff Roster IAW PD Section 6.2.1.	1	LT	NSP	NSP

	PSC: DD01 Schedule and delivery to be determined at the order level.				
				Total Ordering Period 2	**$**

Ordering Period 3: **The Period of Performance shall be from completion of Ordering Period 2 through 365 days after completion of Ordering Period 2. (Actual dates to be provided at award)**					
Line Item	**Description**	**Max QTY**	**Unit**	**Unit Price**	**Extended Price**
		Products			
2001	Firm Fixed Price (FFP) DSS ITM Annual Limited License, Level 1 Facility. DSS-ITM-VA-LL-LVL1 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	51	EA	$	$
2002	FFP DSS ITM Annual Limited License, Level 2 Facility. DSS-ITM-VA-LL-LVL2 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	1	EA	$	$
2003	FFP DSS ITM Annual Limited License, Level 3 Facility. DSS-ITM-VA-LL-LVL3 IAW PD Section 1.3 PSC: DA10	1	EA	$	$

	Schedule and delivery to be determined at the order level.				
2004	FFP DSS ITM Analytics Annual Limited License, per facility. DSS-ITM-Analytics-VA-LL IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	53	EA	$	$
2005	FFP DSS VistA Chemotherapy Manager Large Hospital Annual Limited License. DSS-VCM-LTD-LH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	5	EA	$	$
2006	FFP DSS VistA Chemotherapy Manager Medium Hospital Annual Limited License. DSS-VCM-LTD-MH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	1	EA	$	$
2007	FFP DSS VistA Chemotherapy Manager Small Hospital Annual Limited License. DSS-VCM-LTD-SH IAW PD Section 1.3 PSC: DA10	1	EA	$	$

	Schedule and delivery to be determined at the order level.				
		Services			
2008	FFP DSS Remote Installation Services Per Day. DSS-INST-R IAW PD Section 1.4 PSC: DA10	5	EA	$	$
2009	FFP EMR Technical Installation Services Per Hour. EMRTEC IAW PD Section 1.4 PSC: DA10	40	HR	$	$
2010	FFP DSS Project Management, for new installations, price per hour. PROJ-MGMNT IAW PD Section 1.4 PSC: DD01	225	HR	$	$
2011	FFP EMR Training Per Hour. EMRTRN IAW PD Section 1.4 PSC: U009	1240	HR	$	$
2012	FFP DSS ADHOC Premium Application Workflow Support - Remote, per facility annual fee. DSS-PREMAPPSUPPORT-VAAF IAW PD Section 1.4 PSC: DA10	53	HR	$	$
2013	FFP Travel Expenses Per Person Per Week TRAVEL-Z IAW PD Section 1.4 PSC: V999	150	EA	$	$

2014	FFP DSS Project Management, is for existing installations, Training and Analysis On-Site or Remote. DSS-PROD-SVC IAW PD Section 1.4 PSC: U099	1700	HR	$	$
2015	FFP Conversion of DSS VistA Chemotherapy Manager (VCM) customers to DSS Infusion Therapy Manager (ITM). DSS-ITM-VA Conversion IAW PD Section 1.4 PSC: DA10	1	EA	$	$
2016	FFP DSS VistA Chemotherapy Manager (VCM) Large Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-LH-M IAW PD Section 1.4 PSC: DA10	5	EA	$	$
2017	FFP DSS VistA Chemotherapy Manager Medium Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-MH-M IAW PD Section 1.4 PSC: DA10	1	EA	$	$
2018	FFP DSS VistA Chemotherapy Manager Small Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-SH-M IAW PD Section 1.4 PSC: DA10	1	EA	$	$

2019	Deliverable A: Training Plan and Related Documentation IAW PD Section 1.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
2020	Deliverable A: Master Delivery Schedule IAW PD Section 4.0. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
2021	Deliverable B: Kick-off Meeting Agenda IAW PD Section 4.0 PSC: DD01 Deliverable due within 10 days of task order award.	1	LT	NSP	NSP
2022	Deliverable C: Shipment/Delivery Weekly Progress Report IAW PD Section 4.0. PSC: DD01 Delivery due on a weekly basis upon task order award through close out.	1	EA	NSP	NSP
2023	Deliverable A: Statement of Attestation IAW PD Section 5.7. PSC: DD01	1	LT	NSP	NSP

	Schedule and delivery to be determined at the order level.				
2024	Deliverable A: Compliance Monitoring and Reporting Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
2025	Deliverable B: Corrective Action Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
2026	Deliverable A: AI Model/LLM Change Disclosure IAW PD Section 5.7.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
2027	Deliverable A: Contractor Staff Roster IAW PD Section 6.2.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP

Total Ordering Period 3	**$**

Ordering Period 4:

The Period of Performance shall be from completion of Ordering Period 3 through 365 days after completion of Ordering Period 3. (Actual dates to be provided at award)

Line Item	Description	Max QTY	Unit	Unit Price	Extended Price
	Products				
3001	Firm Fixed Price (FFP) DSS ITM Annual Limited License, Level 1 Facility. DSS-ITM-VA-LL-LVL1 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	30	EA	$	$
3002	FFP DSS ITM Annual Limited License, Level 2 Facility. DSS-ITM-VA-LL-LVL2 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	0	EA	$	$
3003	FFP DSS ITM Annual Limited License, Level 3 Facility. DSS-ITM-VA-LL-LVL3 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	1	EA	$	$

3004	FFP DSS ITM Analytics Annual Limited License, per facility. DSS-ITM-Analytics-VA-LL IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	31	EA	$	$
3005	FFP DSS VistA Chemotherapy Manager Large Hospital Annual Limited License. DSS-VCM-LTD-LH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	1	EA	$	$
3006	FFP DSS VistA Chemotherapy Manager Medium Hospital Annual Limited License. DSS-VCM-LTD-MH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	0	EA	$	$
3007	FFP DSS VistA Chemotherapy Manager Small Hospital Annual Limited License. DSS-VCM-LTD-SH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	0	EA	$	$
Services					

3008	FFP DSS Remote Installation Services Per Day. DSS-INST-R IAW PD Section 1.4 PSC: DA10	0	EA	$	$
3009	FFP EMR Technical Installation Services Per Hour. EMRTEC IAW PD Section 1.4 PSC: DA10	0	HR	$	$
3010	FFP DSS Project Management, for new installations, price per hour. PROJ-MGMNT IAW PD Section 1.4 PSC: DD01	0	HR	$	$
3011	FFP EMR Training Per Hour. EMRTRN IAW PD Section 1.4 PSC: U009	0	HR	$	$
3012	FFP DSS ADHOC Premium Application Workflow Support - Remote, per facility annual fee. DSS-PREMAPPSUPPORT-VAAF IAW PD Section 1.4 PSC: DA10	31	HR	$	$
3013	FFP Travel Expenses Per Person Per Week TRAVEL-Z IAW PD Section 1.4 PSC: V999	70	EA	$	$
3014	FFP DSS Project Management, is for existing installations, Training and Analysis On-Site or Remote. DSS-PROD-SVC	500	HR	$	$

	IAW PD Section 1.4 PSC: U099				
3015	FFP Conversion of DSS VistA Chemotherapy Manager (VCM) customers to DSS Infusion Therapy Manager (ITM). DSS-ITM-VA Conversion IAW PD Section 1.4 PSC: DA10	0	EA	$	$
3016	FFP DSS VistA Chemotherapy Manager (VCM) Large Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-LH-M IAW PD Section 1.4 PSC: DA10	1	EA	$	$
3017	FFP DSS VistA Chemotherapy Manager Medium Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-MH-M IAW PD Section 1.4 PSC: DA10	0	EA	$	$
3018	FFP DSS VistA Chemotherapy Manager Small Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-SH-M IAW PD Section 1.4 PSC: DA10	0	EA	$	$
3019	Deliverable A: Training Plan and Related Documentation IAW PD Section 1.2.	1	LT	NSP	NSP

	PSC: DD01 Schedule and delivery to be determined at the order level.				
3020	Deliverable A: Master Delivery Schedule IAW PD Section 4.0. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
3021	Deliverable B: Kick-off Meeting Agenda IAW PD Section 4.0 PSC: DD01 Deliverable due within 10 days of task order award.	1	LT	NSP	NSP
3022	Deliverable C: Shipment/Delivery Weekly Progress Report IAW PD Section 4.0. PSC: DD01 Delivery due on a weekly basis upon task order award through close out.	1	EA	NSP	NSP
3023	Deliverable A: Statement of Attestation IAW PD Section 5.7. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP

3024	Deliverable A: Compliance Monitoring and Reporting Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
3025	Deliverable B: Corrective Action Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
3026	Deliverable A: AI Model/LLM Change Disclosure IAW PD Section 5.7.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
3027	Deliverable A: Contractor Staff Roster IAW PD Section 6.2.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
				Total Ordering Period 4	**$**

Ordering Period 5:

The Period of Performance shall be from completion of Ordering Period 4 through 365 days after completion of Ordering Period 4. (Actual dates to be provided at award)					
Line Item	**Description**	**Max QTY**	**Unit**	**Unit Price**	**Extended Price**
Products					
4001	Firm Fixed Price (FFP) DSS ITM Annual Limited License, Level 1 Facility. DSS-ITM-VA-LL-LVL1 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	4	EA	$	$
4002	FFP DSS ITM Annual Limited License, Level 2 Facility. DSS-ITM-VA-LL-LVL2 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	0	EA	$	$
4003	FFP DSS ITM Annual Limited License, Level 3 Facility. DSS-ITM-VA-LL-LVL3 IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	0	EA	$	$
4004	FFP DSS ITM Analytics Annual Limited License, per facility. DSS-ITM-Analytics-VA-LL IAW PD Section 1.3 PSC: DA10	4	EA	$	$

	Schedule and delivery to be determined at the order level.				
4005	FFP DSS VistA Chemotherapy Manager Large Hospital Annual Limited License. DSS-VCM-LTD-LH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	0	EA	$	$
4006	FFP DSS VistA Chemotherapy Manager Medium Hospital Annual Limited License. DSS-VCM-LTD-MH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	0	EA	$	$
4007	FFP DSS VistA Chemotherapy Manager Small Hospital Annual Limited License. DSS-VCM-LTD-SH IAW PD Section 1.3 PSC: DA10 Schedule and delivery to be determined at the order level.	0	EA	$	$
Services					
4008	FFP DSS Remote Installation Services Per Day. DSS-INST-R IAW PD Section 1.4 PSC: DA10	0	EA	$	$

4009	FFP EMR Technical Installation Services Per Hour. EMRTEC IAW PD Section 1.4 PSC: DA10	0	HR	$	$
4010	FFP DSS Project Management, for new installations, price per hour. PROJ-MGMNT IAW PD Section 1.4 PSC: DD01	0	HR	$	$
4011	FFP EMR Training Per Hour. EMRTRN IAW PD Section 1.4 PSC: U009	0	HR	$	$
4012	FFP DSS ADHOC Premium Application Workflow Support - Remote, per facility annual fee. DSS-PREMAPPSUPPORT-VAAF IAW PD Section 1.4 PSC: DA10	4	HR	$	$
4013	FFP Travel Expenses Per Person Per Week TRAVEL-Z IAW PD Section 1.4 PSC: V999	8	EA	$	$
4014	FFP DSS Project Management, is for existing installations, Training and Analysis On-Site or Remote. DSS-PROD-SVC IAW PD Section 1.4 PSC: U099	130	HR	$	$
4015	FFP Conversion of DSS VistA Chemotherapy	0	EA	$	$

	Manager (VCM) customers to DSS Infusion Therapy Manager (ITM). DSS-ITM-VA Conversion IAW PD Section 1.4 PSC: DA10				
4016	FFP DSS VistA Chemotherapy Manager (VCM) Large Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-LH-M IAW PD Section 1.4 PSC: DA10	0	EA	$	$
4017	FFP DSS VistA Chemotherapy Manager Medium Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-MH-M IAW PD Section 1.4 PSC: DA10	0	EA	$	$
4018	FFP DSS VistA Chemotherapy Manager Small Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-SH-M IAW PD Section 1.4 PSC: DA10	0	EA	$	$
4019	Deliverable A: Training Plan and Related Documentation IAW PD Section 1.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP

4020	Deliverable A: Master Delivery Schedule IAW PD Section 4.0. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
4021	Deliverable B: Kick-off Meeting Agenda IAW PD Section 4.0 PSC: DD01 Deliverable due within 10 days of task order award.	1	LT	NSP	NSP
4022	Deliverable C: Shipment/Delivery Weekly Progress Report IAW PD Section 4.0. PSC: DD01 Delivery due on a weekly basis upon task order award through close out.	1	EA	NSP	NSP
4023	Deliverable A: Statement of Attestation IAW PD Section 5.7. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
4024	Deliverable A: Compliance Monitoring and Reporting Plan IAW PD Section 5.7.1. PSC: DD01	1	LT	NSP	NSP

	Schedule and delivery to be determined at the order level.				
4025	Deliverable B: Corrective Action Plan IAW PD Section 5.7.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
4026	Deliverable A: AI Model/LLM Change Disclosure IAW PD Section 5.7.2. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
4027	Deliverable A: Contractor Staff Roster IAW PD Section 6.2.1. PSC: DD01 Schedule and delivery to be determined at the order level.	1	LT	NSP	NSP
				Total Ordering Period 5	**$**
				Total Contract Value	**$**

B.3 CONTRACT ADMINISTRATION DATA

1. Contract Administration: All contract administration matters will be handled by the following individuals:

a. CONTRACTOR:

TBD

b. GOVERNMENT:

Contracting Officer 36C10A
Department of Veterans Affairs
Technology Acquisition Center
23 Christopher Way
Eatontown NJ 07724

2. CONTRACTOR REMITTANCE ADDRESS: All payments by the Government to the contractor will be made in accordance with:

[X] 52.232-33, Payment by Electronic Funds Transfer—System For Award Management, or
[] 52.232-36, Payment by Third Party

3. INVOICES: Invoices shall be submitted in arrears:

a. Quarterly []

b. Semi-Annually []

c. Other [X] Upon acceptance of Deliverables, In accordance with (IAW) Section B.2 Price Schedule

4. GOVERNMENT INVOICE ADDRESS: All Invoices from the contractor shall be submitted electronically in accordance with VAAR Clause 852.232-72 Electronic Submission of Payment Requests.

ACKNOWLEDGMENT OF AMENDMENTS: The offeror acknowledges receipt of amendments to the Solicitation numbered and dated as follows:

AMENDMENT NO	DATE

B.4 GOVERNING LAW

Federal law and regulations, including the Federal Acquisition Regulations (FAR), shall govern this Contract/Order. Commercial license agreements may be made a part of this Contract/Order but only if both parties expressly make them an addendum hereto. If the commercial license agreement is not made an addendum, it shall not apply, govern, be a part of or have any effect whatsoever on the Contract/Order; this includes, but is not limited to, any agreement embedded in the computer software (clickwrap), any agreement that is otherwise delivered with or provided to the Government with the commercial computer software or documentation (shrinkwrap), or any other license agreement otherwise referred to in any document. If a commercial license agreement is made an addendum, only those provisions addressing data rights regarding the Government's use, duplication and disclosure of data (e.g., restricted computer software) are included and made a part of this Contract/Order, and only to the extent that those provisions are not duplicative or inconsistent with Federal law, Federal regulation, the incorporated FAR clauses and the provisions of this Contract/Order; those provisions in the commercial license agreement that do not address data rights regarding the Government's use, duplication and disclosure of data shall not be included or made a part of the Contract/Order. Federal law and regulation including, without limitation, the Contract Disputes Act (41 U.S.C. § 7101 et seq.), the Anti-Deficiency Act (31 U.S.C. § 1341 et seq.), the Competition in Contracting Act (41 U.S.C. § 3301 et seq.), the Prompt Payment Act (31 U.S.C. § 3901 et seq.), Contracts for Data Processing or Maintenance (38 USC § 5725), Source Code Harmonization and Reuse in Information Technology Act "SHARE IT Act" (P.L. 118-187), and RFO FAR clauses RFO 52.212-4, RFO 52.227-14 shall supersede, control, and render ineffective any inconsistent, conflicting, or duplicative provision in any commercial license agreement. In the event of conflict between this clause and any provision in the Contract/Order or the commercial license agreement or elsewhere, the terms of this clause shall prevail. The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by RFO 52.227-14, this includes any custom code developed for the purpose of performing under this contract. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ) in accordance with 28 U.S.C. § 516; at the discretion of DOJ, the Contractor may be allowed reasonable participation in the defense of the litigation. Any additional changes to the Contract/Order must be made by modification (Standard Form 30) and shall only be made by a warranted Contracting Officer. Nothing in this Contract/Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

B.5 SOFTWARE LICENSE, MAINTEANCE AND TECHNICAL SUPPORT

(1). Definitions.

a) Licensee. The term “licensee” shall mean the U.S. Department of Veterans Affairs (“VA”) and is synonymous with “Government.”
b) Licensor. The term “licensor” shall mean the Contractor having the necessary license or ownership rights to deliver license, software maintenance and support of the computer software being acquired. The term “Contractor” is the party identified in Block 17a on the SF1449. If the Contractor is a reseller and not the Licensor, the Contractor remains responsible for performance under this Contract/Order.
c) Software. The term “software” shall mean the licensed computer software product(s) cited in the Schedule of Supplies/Services.
d) Maintenance. The term “maintenance” is the process of enhancing and optimizing software, as well as remedying defects. It shall include all new fixes, patches, releases, updates, versions and upgrades, as further defined below.
e) Technical Support. The term “technical support” refers to the range of services providing assistance for the software via the telephone, email, a website or otherwise.
f) Release or Update. The term “release” or “update” are terms that refer to a revision of software that contains defect corrections, minor enhancements or improvements of the software’s functionality. This is usually designated by a change in the number to the right of the decimal point (e.g., from Version 5.3 to 5.4). An example of an update is the addition of new hardware.
g) Version or Upgrade. The term “version” or “upgrade” are terms that refer to a revision of software that contains new or improved functionality. This is usually designated by a change in the number to the left of the decimal point (e.g., from Version 5.4 to 6).

(2). Software License.

a) Unless otherwise stated in the Schedule of Supplies/Services, the Performance Work Statement or Product Description, the software license provided to the Government is a perpetual, nonexclusive license to use the software.
b) The Government may use the software in a networked environment.
c) Any dispute regarding the license grant or usage limitations shall be resolved in accordance with the Disputes Clause incorporated in FAR 52.212-4(d).
d) All limitations of software usage are expressly stated in the Schedule of Supplies/Services and the Performance Work Statement/Product Description.

(3). Software Maintenance and Technical Support.

a) If the Government desires to continue software maintenance and support beyond the period of performance identified in this Contract/Order, the Government will issue a separate contract or order for maintenance and support. Conversely, if a contract or order for continuing software maintenance and technical support is not received, the Contractor is neither authorized nor permitted to renew any of the previously furnished services.
b) The Contractor shall provide software support services, which includes periodic updates, enhancements and corrections to the software, and reasonable technical support, all of which are customarily provided by the Contractor to its commercial customers so as to cause the software to perform according to its specifications, documentation or demonstrated claims.
c) Any telephone support provided by Contractor shall be at no additional cost.
d) The Contractor shall provide all maintenance services in a timely manner in accordance with the Contractor's customary practice or as defined in the Performance Work Statement or Product Description. However, prolonged delay (exceeding 2 business days) in resolving software problems will be noted in the Government's various past performance records on the Contractor (e.g., www.cpars.gov).
e) If the Government allows the maintenance and support to lapse and subsequently wishes to reinstate it, any reinstatement fee charged shall not exceed the amounts that would have been charged if the Government had not allowed the subscription to lapse.

(4). Disabling Software Code. The Government requires delivery of computer software that does not contain any code that will, upon the occurrence or the nonoccurrence of any event, disable the software. Such code includes but is not limited to a computer virus, restrictive key, node lock, time-out or other function, whether implemented by electronic, mechanical, or other means, which limits or hinders the use or access to any computer software based on residency on a specific hardware configuration, frequency of duration of use, or other limiting criteria. If any such disabling code is present, the Contractor agrees to indemnify the Government for all damages suffered as a result of a disabling caused by such code, and the contractor agrees to remove such code upon the Government's request at no extra cost to the Government. Inability of the Contractor to remove the disabling software code will be considered an inexcusable delay and a material breach of contract, and the Government may exercise its right to terminate for cause. In addition, the Government is permitted to remove the code as it deems appropriate and charge the Contractor for consideration for the time and effort expended in removing the code.

(5). Manuals and Publications. Upon Government request, the Contractor shall furnish the most current version of the user manual and publications for all products/services provided under this Contract/Order at no cost.

B.6 ACCOUNTING AND APPROPRIATION DATA

Funds in the amount of $TBD are obligated on Purchase Order Number TBD to fund Contracting Line Item Number(s) TBD to fulfill the minimum order guarantee.

The contractor shall reference the Purchase Order Number on each invoice submitted for payment.

B.7 ORDERING PROCEDURES

a. Orders against this IDIQ contract will be issued in accordance with its terms and conditions at the sole discretion of the Government by a VA Contracting Officer during the period of the award date through 60 months thereafter. Individual delivery orders may include options for extended terms. Performance is authorized under any order issued against this IDIQ for up to 12 months after the end of the last ordering period. Upon receipt of a delivery order, the Contractor shall provide services at the prices set forth in the Schedule;

b. Orders issued will be Firm Fixed Price. Each order is a stand-alone order, with individual periods of performance.

B.8 PRODUCT DESCRIPTION

1.0 PRODUCT REQUIREMENTS

1.1 Background

The Department of Veterans Affairs (VA), Veterans Health Administration, National Oncology Program Office requires Document Storage Systems (DSS) Infusion Therapy Manager (ITM) software and associated services for any of the VA Medical Centers (VAMC) across the United States. The solution must be interoperable and compatible for use with the Veterans Health Information Systems and Technology Architecture (VistA) and the Computerized Patient Record System (CPRS) which is a graphical user interface (GUI) for the VistA electronic health record (EHR) system. VA requires brand name DSS ITM for sites using VistA Chemotherapy Manager (VCM), the pre-existing legacy version of DSS ITM, to manage infusion therapy in CPRS/VistA that has not yet transitioned to the new Oracle EHR. Each of these sites shall have the ability to utilize the national contract for DSS ITM software since DSS is retiring the pre-existing contracted VCM software for ordering antineoplastic and other infusion therapy in VistA/CPRS and is replacing VCM with its next-generation solution, ITM, which is also compatible with VistA/CPRS. Examples of required interfaces with CPRS/VistA include patient specific information which includes labs, age, height, to calculate patient specific doses, allergy alerts, and dose alerts. In addition, a requirement of the system is to document in CPRS/VistA detailing the patient specific chemotherapy regimen including doses and dates. Another required functional capability of the system is placing the medication orders directly into VISTA with minimal editing.

Procurement of ITM software provides tools for VA Medical Centers (VAMCs) utilizing the VistA/CPRS EHR system to standardize the antineoplastic and other infusion therapy treatment protocols and provider order entry available for patient care. The application provides antineoplastic and other infusion therapy management functionality for specialty care areas (including but not limited to oncology, gastroenterology, rheumatology, neurology, and endocrinology) and pharmacy. Interfaces must be available to the patient’s VistA profile, Admit/Discharge/Transfer (ADT) registration for demographics and visit status, Laboratory, Pharmacy, Allergies, and Vitals data from VistA to ITM. Implementation and application training services should be available for orderable item verification, administration, treatment plan building, general user, superuser and mentoring during go live. Technical and general support services must be provided throughout the Period of Performance (PoP).

In accordance with VHA Directive 1415 and the American Society of Clinical Oncology and Oncology Nursing Society (ASCO-ONS) Antineoplastic Therapy Administration Safety Standards, use of such software in VistA/CPRS improves safety by reducing transcription errors through electronic ordering when available as well as through ordering whole treatment regimens together (e.g., medications to be given pre- and post- treatment in addition to primary treatment medication). The ITM software features custom order sets, based on clinical guidelines, to be tailored to each facility’s preferences by their subject matter experts (SMEs), including in oncology, gastroenterology, rheumatology, neurology, endocrinology, and clinical pharmacy. The ITM software combines comprehensive end-to-end automation of complex antineoplastic and other infusion therapy ordering based on evidence-based treatment plans. The software streamlines workflows for antineoplastic therapy, immunotherapy,

hydration, antibiotics, and other infusion therapies. These features assist medical staff in order entry, as well as the standardization of practices with the latest clinical evidence through decision support.

Approximately 120 VAMCs provide antineoplastic therapy and approximately 50 VAMCs utilize the soon-to-be retired VCM software. Salt Lake City VAMC, a previous VCM user, currently has an ITM software contract in place and already went live with the conversion from VCM to ITM in 2025. Mountain Home, TN VAMC also went live with ITM in February 2026. Until the Oracle EHR system, replacing VistA/CPRS, is implemented at all VAMCs (scheduled for completion by November 2031), there is an enterprise-wide immediate need for this web-enabled software application for VistA/CPRS users to facilitate organizational initiatives to:

• Automate antineoplastic and other infusion therapy management and ordering

• Enable standardization of antineoplastic and other infusion therapy approaches and accompaniments

• Reduce costs of administration of antineoplastic and other infusion therapies

Once the Oracle EHR system goes live at a VAMC, this contract will no longer be utilized for that specific VAMC.

1.2 Functional Requirements

Contractor shall provide licenses, configuration, installation, and remote technical support for Brand name DSS ITM software. Installation consists of project management and remote installation services. Contractor shall work with the VHA and Commercial Off-The-Shelf (COTS) teams to install ITM software and provide Installation manuals to users and COTS teams prior to the Installation date. The DSS Installation team will complete both test and production server installations of the software. Vendor must coordinate with the facility to install ITM on hospital provided servers and appropriate clinical workstations.

Implementation by the Contractor must encompass:

- ITM in the Oncology, Gastroenterology, Rheumatology, Neurology, Endocrinology, Infusion clinic, Inpatient, and Pharmacy settings of the facility.
- Education and training to ensure users know how to provide orderable item verification and treatment plan building, as well as general user and administrative functions.
- Education and training on how to upload or build treatment plans in ITM to meet each facility standard of care.
- Education and training sessions for testing and production use.
- On-site support during go-live implementation.
- System and user documentation.
- Contractor Project Management Plans (CPMPs)
- Contingency plans.
- Training plans and educational materials.
- Post-implementation support plan.

Contractor must develop and deliver education, including a training plan and related documentation (e.g., training materials, installation manuals, user guides, on-line courses, training assessments, and course evaluations) for each project developed and delivered based on scope, stakeholders (OI&T, super-users, CACs/ADPAC, RNs, Pharmacists, MDs, etc.), and environment, providing follow-up support as needed.

Contractor shall provide technical services and support, working with OI&T, Biomedical Engineering, and VHA staff to provide the needs to sustain all the capabilities, features, and functions of the solution to ensure that it will be operable, available for use and responsive to user commands and entries.

The FFP travel requirement is for travel expenses only. The labor associated with the installation and training shall only be covered by the specific installation and training Contracting Line Item Numbers.

This action is for a comprehensive National DSS ITM IDIQ contract that shall include VAMCs across the VA enterprise. Products and services shall be available to any VAMC, that has not transitioned to the Oracle HER. Deployment of DSS ITM in VA is local with on-premises VA/VISN servers that connect to facility VistA databases. VA will determine via task order the requirements for a single software installation. Support for software installations will be closely coordinated with the VA Contracting Officer's Representative (COR) and the local facility. There is no development work under this effort.

Deliverables:

A. Training Plan and Related documentation (as described above)

The following Products and Service Tables provide estimates for each year. See Price Schedule for maximum quantities for each item.

1.3 Products

Description/Part Number	Order Per 1	Order Per 2	Order Per 3	Order Per 4	Order Per 5
DSS Infusion Therapy Manager (ITM) Annual Limited License, Level 1 Facility. DSS-ITM-VA-LL-LVL1	50	65	51	30	4
DSS Infusion Therapy Manager (ITM) Annual Limited License, Level 2 Facility. DSS-ITM-VA-LL-LVL2	5	4	1	0	0
DSS Infusion Therapy Manager (ITM) Annual Limited License, Level 3 Facility. DSS-ITM-VA-LL-LVL3	7	6	1	1	0
DSS Infusion Therapy Manager (ITM) Analytics Annual Limited License, per facility. DSS-ITM-Analytics-VA-LL	62	75	53	31	4

DSS VistA Chemotherapy Manager Large Hospital Annual Limited License. DSS-VCM-LTD-LH	5	5	5	1	0
DSS VistA Chemotherapy Manager Medium Hospital Annual Limited License. DSS-VCM-LTD-MH	1	1	1	0	0
DSS VistA Chemotherapy Manager Small Hospital Annual Limited License. DSS-VCM-LTD-SH	1	1	1	0	0

1.4 Services

Description/Part Number	Order Per 1	Order Per 2	Order Per 3	Order Per 4	Order Per 5
DSS Remote Installation Services Per Day. DSS-INST-R	62	10	5	0	0
EMR Technical Installation Services Per Hour. EMRTEC	500	80	40	0	0
DSS Project Management, price per hour. PROJ-MGMNT	2750	450	225	0	0
EMR Training Per Hour. EMRTRN	15400	2480	1240	0	0
DSS ADHOC Premium Application Workflow Support - Remote, per facility annual fee. DSS-PREMAPPSUPPORT-VAAF	62	75	53	31	4
Travel Expenses Per Person Per Week TRAVEL-Z	750	200	150	70	8
DSS Project Management, Training and Analysis, On-Site or Remote. DSS-PROD-SVC	160	1900	1700	500	130
Conversion of DSS VistA Chemotherapy Manager (VCM) customers to DSS Infusion Therapy Manager (ITM). DSS-ITM-VA Conversion	14	2	1	0	0
DSS VistA Chemotherapy Manager (VCM) Large Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-LH-M	5	5	5	1	0
DSS VistA Chemotherapy Manager Medium Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-MH-M	1	1	1	0	0
DSS VistA Chemotherapy Manager Small Hospital Software Subscription Maintenance and Support. DSS-VCM-PERP-SH-M	1	1	1	0	0

2.0 NOTICE OF THE FEDERAL ACCESSIBILITY LAW AFFECTING ALL INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) PROCUREMENTS (SECTION 508)

On January 18, 2017, the Access Board issued a final rule that updated accessibility requirements covered by Section 508 and refreshed guidelines for telecommunications equipment subject to Section 255 of the Communications Act. The final rule went into effect on January 18, 2018. The revisions and updates to the Section 508-based standards and Section 255-based guidelines are intended to ensure that information and communication technology (ICT) covered by the respective statutes is accessible to and usable by individuals with disabilities.

2.1 SECTION 508 – INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) STANDARDS

The Section 508 standards established by the Access Board are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure ICT. These standards are found in their entirety at: Revised 508 Standards and 255 Guidelines (access-board.gov). A single PDF file version of the Revised Section 508 Standards and 255 Guidelines will be supplied upon request, or can be obtained from the Access Board website. Federal agencies must comply with the Rehabilitation Act of 1973, as amended.

The Contractor shall comply with “508 Chapter 2: Scoping Requirements” for all electronic ICT and content delivered under this contract. Specifically, as appropriate for the technology and its functionality, the Contractor shall comply with the technical standards marked here:

- ☐ E205 Electronic Content – (Accessibility Standard -WCAG 2.0 Level A and AA Guidelines)
- ☒ E204 Functional Performance Criteria
- ☒ E206 Hardware Requirements
- ☒ E207 Software Requirements
- ☒ E208 Support Documentation and Services Requirements

2.2 COMPATABILITY WITH ASSISTIVE TECHNOLOGY

The standards do not require installation of specific accessibility-related software or attachment of an assistive technology device. Section 508 requires that ICT be compatible with such software and devices so that ICT can be accessible to and usable by individuals using assistive technology, including but not limited to screen readers, screen magnifiers, and speech recognition software.

2.3 ACCEPTANCE AND ACCEPTANCE TESTING

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the Section 508 Chapter 2: Scoping Requirements standards identified above.

The Government reserves the right to test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

3.0 INFORMATION TECHNOLOGY USING SUSTAINABLE PRODUCTS

The Contractor shall comply with Sections 524 and Sections 525 of the Energy Independence and Security Act of 2007; Section 104 of the Energy Policy Act of 2005; Executive Order 14148, "Initial Rescissions of Harmful Executive Orders and Actions," dated January 20, 2025; Executive Order 13221, "Energy-Efficient Standby Power Devices," dated August 2, 2001; and the Revolutionary Federal Acquisition Regulation (FAR) Overhaul (RFO) to provide ENERGY STAR® certified and Federal Energy Management Program (FEMP) Designated Low Standby Power information technology products, see https://www.energy.gov/femp/search-energy-efficient-products. See http://www.energystar.gov for complete product specifications and updated lists of Energy Star certified products. FEMP low standby power product listing can be found at https://www.energy.gov/femp/low-standby-power-product-list.

The Contractor shall provide products that meet the definition of sustainable products if the products are delivered to the Government; furnished by the Contractor for use by the Government, incorporated into the construction of a public building or public work, or acquired by the Contractor for use in performing services under a Government contract where the cost of the products is a direct cost to a Government contract (versus costs which are normally applied to a contractor's general and administrative expenses or indirect costs).

Specifically, the Contractor shall provide sustainable products under this contract in accordance with RFO 52.223-23 (NOV 2025). The applicable products with their associated certification and/or designation required (e.g. Energy Star, FEMP Low Standby Power) are identified within the product requirements specifications in this PD. The Contractor shall self-certify that its proposed products meet the certification(s) and/or designation(s) specified.

4.0 SHIPMENT OF HARDWARE OR EQUIPMENT

The Contractor shall complete the Master Delivery Schedule in accordance with the Instructions, and shall coordinate with the COR for specifics. The Master Delivery Schedule shall be provided after award and updated prior to and after each delivery timeframe.

Deliverable:

A: Master Delivery Schedule

Shipment/Delivery Kick-off Meeting

The Contractor shall conduct a Shipment/Delivery Kick-off Meeting with the VA Program Manager (PM), COR, Delivery Date Coordinator, Implementation Manager, and Facility CIOs (or designee) to discuss at a minimum: the delivery schedule requirements, high-level implementation overview and schedule, the invoicing requirements and facilitate delivery of equipment. This meeting may be held in conjunction with the post award conference or identified technical kickoff meeting, if applicable. The Contractor shall also present the Shipment/Delivery Weekly Progress Report format for review and approval by the Government. This meeting, shall be scheduled within ten days for each site after award and the agenda shall be provided at this time.

Deliverable:

B: Kick-off Meeting Agenda

Shipment/Delivery Weekly Progress Report

The Contractor shall provide a Shipment/Delivery Weekly Progress Report which shall identify the items shipped, the serial number associated with each piece of equipment; the date of each shipment; the status of each shipment, tracking information, and information relative to Government-receipt of the equipment items at each delivery site. In addition, the Shipment/Delivery Weekly Progress Report shall identify any problems and provide a description of how the problems were resolved/addressed. If problems have not been completely resolved, the Contractor shall provide an explanation and status of resolution. Shipment/Delivery Weekly Progress Reports shall be submitted in Microsoft Excel Format and shall clearly identify each serial number of the equipment being delivered with one (1) serial number per cell.

Deliverable:

C: Shipment/Delivery Weekly Progress Report

Inspection: Destination
Acceptance: Destination
Free on Board (FOB): Destination

Packing Slips/Labels and Lists shall also include the following:

IFCAP PO #: _____ (e.g., 166-E11234 (the IFCAP PO number is located in block #20 of the SF 1449))

Project Description: (e.g. Tier 1 Lifecycle Refresh)

Total number of Containers: Package ___ of ___. (e.g., Package 1 of 3)

5.0 GENERAL REQUIREMENTS

5.1 VA TECHNICAL REFERENCE MODEL

The Contractor shall comply with the VA OIT Technical Reference Model (VA TRM). Compliance with the VA TRM is achieved by using only technologies and standards that are listed as approved for use in the VA TRM. The Contractor shall provide all necessary information requested by VA to ensure TRM approval is obtained prior to use on VA's network.

5.2 ZERO TRUST – VA CRITICAL SECURITY CONTROLS

VA has established minimum mandatory security requirements and requires that any network connected software system or service must meet the VA Critical Security Controls as outlined in the VA Memorandum, "VA Security Controls", https://www.voa.va.gov/DocumentView.aspx?DocumentID=5010. VA Critical Security Controls identify the minimum mandatory requirements that must be implemented across all VA enterprise infrastructure, cloud computing environments, information systems, networks, and specialized devices (medical devices/systems, special-purpose systems, and research scientific computing devices) that process, store, and/or transmit VA data. Effective July 1, 2025, the Contractor shall implement these VA Critical Security Controls, within any network connected software system or service prior to being authorized for use in the VA. This functional requirement is not negotiable, and Plan of Action & Milestones (POAM) will not be accepted in the event these controls

cannot be implemented for new systems. Critical Security Controls are intended to increase VA's security posture and provide security and privacy risk visibility into the VA network and is not a new requirement. The Contractor's failure to maintain these VA Critical Controls after implementation will result in VA discontinuing the use of the system.

5.3 SOCIAL SECURITY NUMBER (SSN) REDUCTION

The Contractor solution shall support the Social Security Number (SSN) Fraud Prevention Act (FPA) of 2017 which prohibits the inclusion of SSNs on any document sent by mail. The Contractor support shall also be performed in accordance with Section 240 of the Consolidated Appropriations Act (CAA) 2018, enacted March 23, 2018, which mandates VA to discontinue using SSNs to identify individuals in all VA information systems as the Primary Identifier. The Contractor shall ensure that any new IT solution discontinues the use of SSN as the Primary Identifier to replace the SSN with the Integrated Control Number (ICN) in all VA information systems for all individuals. The Contractor shall ensure that all Contractor delivered applications and systems integrate with the VA Master Person Index (MPI) for identity traits to include the use of the ICN as the Primary Identifier. The Contractor solution may only use a Social Security Number to identify an individual in an information system if and only if the use of such number is required to obtain information VA requires from an information system that is not under the jurisdiction of VA.

5.4 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support IPv6-Only based upon the memo issued by the Office of Management and Budget (OMB) on November 19, 2020 (https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-07.pdf). Which defines IPv6-only as the state of an operational system or service when IPv4 protocol functions (addressing, packet forwarding) are not in use. The NIST USGv6 profile defines technical requirements for a product to be capable of operating in IPv6-Only environments. IPv6-Only technology, in accordance with the USGv6 Program (https://www.nist.gov/programs-projects/usgv6-program/usgv6-revision-1), NIST Special Publication (SP) 500-267B Revision 1 "USGv6 Profile" (https://doi.org/10.6028/NIST.SP.500-267Br1), and NIST SP 800-119 "Guidelines for the Secure Deployment of IPv6" (https://doi.org/10.6028/NIST.SP.800-119), compliance shall be included in all IT infrastructures, application designs, application development, operational systems and sub-systems, and their integration. In addition to the above requirements, all devices, applications, and systems shall support all applicable functionality on native IPv6-Only as well as dual stack (IPv6 / IPv4) connectivity without additional memory or other resources being provided by the Government, so that they can function in a mixed environment. All public/external facing servers and services (e.g., web, email, DNS, ISP services, etc.) shall support native IPv6-Only and dual stack (IPv6 / IPv4) users and all internal infrastructure and applications shall support using native IPv6-Only and dual stack (IPv6 / IPv4) for all functionality and operations.

5.5 SOFTWARE AND LICENSING REQUIREMENTS

The Contractor shall be responsible for the provision of all software licenses and any associated licensing maintenance required for any development, delivery, integration, operation, and/or maintenance associated with its proposed application(s), software products, software solution, and/or system including, but not limited to, any and all

application(s), software and/or software products that comprise, are a part of, or integrate with the Contractor's proposed application(s), software products, software solution, and/or system for the life of any resulting contract.

5.6 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M-19-26, "Update to the Trusted Internet Connections (TIC) Initiative" (https://www.whitehouse.gov/wp-content/uploads/2019/09/M-19-26.pdf), VA Directive 6513 "Secure External Connections", and shall comply with the TIC 3.0 Core Guidance Documents, including all Volumes and TIC Use Cases, found at the Cybersecurity & Infrastructure Security Agency (CISA) (https://www.cisa.gov/publication/tic-30-core-guidance-documents.)

5.7 GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS

If Artificial Intelligence (AI) is part of the Contractor system/solution, the Contractor shall be in compliance with E.O. 13960 and 14319, OMB Memorandums M-25-21, M-25-22, and M-26-04, and VA Directive and Handbook 6500 to support VA in trustworthy, secure, responsible, accountable, Truth Seeking, and Ideologically Neutral AI innovation.

No web-based, publicly available generative AI service has been approved for use with VA-sensitive data including, but not limited to OpenAI's ChatGPT, Microsoft's Copilot, Google's Gemini, and Anthropic's Claude. No PII, protected health information (PHI), or VA-sensitive data should be entered into these unapproved services. The entire definition of VA Sensitive Data can be found at 38 U.S.C. § 5727 (23). The Contractor shall protect VA Sensitive data from unauthorized disclosure or use, and from being used to train or improve the functionality of the vendor's commercial offerings without express permission from VA.

The Contractor shall deliver the services, technical data, configurations, models, weights, documentation or other information, including source code, developed during contract performance. The Contractor, in collaboration with VA, must evaluate the output of any AI tool for accuracy prior to using the output in VA efforts. All data, including models, weights, algorithms, and outputs generated using either Government-furnished data or data first developed under this contract shall be the property of the Government with unlimited rights as defined by FAR 52.227-14. The Contractor shall also deliver any custom-developed code developed with AI methodologies in accordance with the SHARE IT Act, if applicable. VA shall also retain unlimited rights to any improvements to that data, including the continued design, development, testing, and operation of AI systems and/or systems utilizing AI.

The Contractor shall ensure that all AI Systems, including Large Language Models (LLM), whether standalone LLMs or integrated into broader software platforms, procured under this effort and/or used in performance of this contract complies with the Unbiased AI Principles as defined in Executive Order 14319 and OMB Memorandum M-26-04, e.g. Truth Seeking and Ideologically Neutral, as applicable to the intended use of the system.

The Contractor shall ensure that AI System/LLM generated outputs are truthful in responding to user prompts seeking factual information or analysis, prioritize historical

accuracy, scientific inquiry, and objectivity, as well as acknowledge uncertainty where reliable information is incomplete or contradictory and do not fabricate, hallucinate, or present unverifiable information as fact.

The Contractor shall ensure that LLMs and AI outputs are neutral, nonpartisan tools that do not manipulate responses in favor of ideological dogmas such as Diversity, Equity, and Inclusion (DEI). The Contractor shall ensure that the LLMs, including the AI System, are not intentionally encoded with partisan or ideological judgments within an AI System's/LLM's outputs unless those judgments are prompted by or otherwise readily accessible to the end user.

Compliance with the AI requirements of this contract, including adherence to the Unbiased AI Principles, Truth-Seeking and Ideological Neutrality requirements, disclosure obligations, monitoring and reporting requirements, and corrective action responsibilities, is a material condition of eligibility for payment and continued performance. In accordance with OMB Memorandum M-26-04, failure to comply with these requirements, or refusal to take timely and appropriate corrective action to remedy identified noncompliance, may constitute a material breach of contract and may result in remedies consistent with the terms of the contract and applicable law including but not limited to withholding of payment, termination for cause/default, or other appropriate contractual remedies, as determined by the Contracting Officer.

All AI for delivery and/or use in performance of the contract shall adhere to the *VA Trustworthy AI Framework*, available at https://department.va.gov/ai/trustworthy/. Once the Contractor has obtained CO authorization to use specific AI in contract performance, the Contractor shall provide the COR a signed Statement of Attestation prior to AI implementation as identified in the Artificial Intelligence in VA Contracts clause, to include its associated list of AI being used in contract performance.

Deliverable:

A. Statement of Attestation

5.7.1 MONITORING, REPORTING, AND CORRECTIVE ACTION

The Contractor shall develop and implement a Compliance Monitoring and Reporting Plan supporting ongoing monitoring processes to evaluate AI outputs for compliance with Trustworthy AI and Unbiased AI principles. This plan shall include the mechanism for authorized users to provide end user feedback to report suspected violations of Truth-Seeking or Ideological Neutrality requirements.

The Contractor shall notify the COR within 10 business days of identifying any material deviation from these principles and shall submit a written Corrective Action Plan describing mitigation steps, responsible parties, and timelines. Any material deviation, corrective action taken, and results shall be detailed in the Monthly Progress Reports.

Deliverable:

A. Compliance Monitoring and Reporting Plan
B. Corrective Action Plan

5.7.2 AI MODEL UPDATES AND CHANGE DISCLOSURES

The Contractor, in an AI Model/LLM Change Disclosure, shall notify the Government throughout the PoP in advance of any material changes to AI models, including new AI enhancements, features and/or components, controls, retraining, classifiers, system prompts, fine-tuning, content moderation, filters, version replacement, or architectural changes, that could reasonably affect compliance with Trustworthy AI or Unbiased AI principles. Updated documentation shall be provided to VA for VA approval prior to implementation of such changes.

Deliverable:

A. AI Model/LLM Change Disclosure

6.0 SECURITY AND PRIVACY REQUIREMENTS

6.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

In accordance with VA Handbook 0710, Personnel Vetting Program, the position sensitivity and the level of background investigation commensurate with the required level of access for the following tasks within the PD are:

Position Sensitivity and Background Investigation Requirements by Service Task/Item Number

Service Task / Item Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
1.1	☒	☐	☐
1.2	☒	☐	☐

The Tasks identified above and the resulting Position Sensitivity and Background Investigation requirements identify, in effect, the Background Investigation requirements for Contractor individuals, based upon the tasks the particular Contractor individual will be working. The submitted Contractor Staff Roster must indicate the required Background Investigation Level for each Contractor individual based upon the tasks the Contractor individual will be working, in accordance with their submitted proposal.

6.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

6.2.1 Responsibilities:

a. The Contractor shall prescreen all personnel requiring access to the computer systems to ensure they maintain the appropriate Background Investigation, and are able to read, write, speak, and understand the English language.
b. Within 3 business days after award, the Contractor shall provide a roster of Contractor and Subcontractor employees to the COR to begin their background investigations in accordance with the PAL template artifact. The Contractor Staff Roster shall contain the Contractor's Full Name, Date of Birth, Place of Birth, individual background investigation level requirement (based upon Section 6.2.1 Tasks), etc. The Contractor shall submit full Social Security Numbers either within the Contractor Staff Roster or under separate cover to the COR. The Contractor Staff Roster shall be updated and provided to VA within 1 day of any changes in employee status, training certification

completion status, Background Investigation level status, additions/removal of employees, etc. throughout the Period of Performance. The Contractor Staff Roster shall remain a historical document indicating all past information and the Contractor shall indicate in the Comment field, employees no longer supporting this contract. The preferred method to send the Contractor Staff Roster or Social Security Number is by encrypted e-mail. If unable to send encrypted e-mail, other methods which comply with FIPS 140-2 (or its successor) are to encrypt the file, use a secure fax, or use a traceable mail service. (Note that by September 22, 2026, all FIPS 140-2 certificate validations will be placed on the Historical List. See FIPS Transition Effort Timeline for more details: https://csrc.nist.gov/projects/fips-140-3-transition-effort#schedule)

c. The Contractor should coordinate with the location of the nearest VA fingerprinting office through the COR. Only electronic fingerprints are authorized. The Contractor shall bring their completed Personnel Security Adjudication Center (PSAC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.
d. The Contractor shall ensure the following required forms are submitted to the COR within 5 days after contract award:
    1) Optional Form 306
    2) Self-Certification of Continuous Service
    3) VA Form 0710
    4) Completed PSAC Fingerprint Request Form
e. The Contractor personnel shall submit all required information related to their background investigations (completion of the investigation documents (SF85, SF85P, or SF 86) utilizing the Defense Counterintelligence and Security Agency (DCSA) National Background Investigation Services (NBIS) Electronic Application (eAPP) (formerly e-QIP) after receiving an email notification from the PSAC.
f. The Contractor employee shall certify and release the eAPP document, print, and sign the signature pages, and send them encrypted to the COR for electronic submission to the PSAC. These documents shall be submitted to the COR within 3 business days of receipt of the eAPP) notification email. (Note: DCSA is moving towards a “click to sign” process. If click to sign is used, the Contractor employee should notify the COR within 3 business days that documents were signed via eAPP).
g. The Contractor shall be responsible for the actions of all personnel provided to work for VA under this contract. In the event that damages arise from work performed by Contractor provided personnel, under the auspices of this contract, the Contractor shall be responsible for all resources necessary to remedy the incident.
h. A Contractor may be granted unescorted access to VA facilities and/or access to VA Information Technology resources (network and/or protected data) with a favorably adjudicated Special Agreement Check (SAC), completed training delineated in VA Handbook 6500.6 (Appendix C, Section 4), signed “Contractor Rules of Behavior”, and with a valid, operational Personal Identity Verification (PIV) credential for PIV-only logical access to VA’s network. A PIV card credential can be issued once your SAC has been favorably adjudicated and your background investigation has been scheduled

by DCSA. However, the Contractor will be responsible for the actions of the Contractor personnel they provide to perform work for VA. The investigative history for Contractor personnel working under this contract must be maintained in the database of DCSA.

i. The Contractor, when notified of an unfavorably adjudicated background investigation on a Contractor employee as determined by the Government, shall withdraw the employee from consideration in working under the contract.
j. Failure to comply with the Contractor personnel security investigative requirements may result in loss of physical and/or logical access to VA facilities and systems by Contractor and Subcontractor employees and/or termination of the contract for default.
k. PIV Credential Holders must follow all HSPD-12 policies and procedures as well as use and protect their assigned identity credentials in accordance with VA policies and procedures, displaying their badges at all times, and returning the identity credentials upon termination of their relationship with VA.

Deliverable:

A. Contractor Staff Roster

ADDENDUM B – VA INFORMATION AND INFORMATION SYSTEM SECURITY/ PRIVACY LANGUAGE

NOTE: In the event of a conflict, VA Acquisition Regulation (VAAR) Security Clauses take precedence over the language in this Addendum B.

APPLICABLE SECTIONS TAILORED FROM: *VA NOTICE 24-12, APRIL 22, 2024, UPDATE TO VA HANDBOOK 6500.6, CONTRACT SECURITY, APPENDIX C VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE, FOR INCLUSION INTO CONTRACTS, AS APPROPRIATE*

B1. GENERAL

This entire section applies to all acquisitions requiring any Information Security and Privacy language. Contractors, contractor personnel, Subcontractors and subcontractor personnel will be subject to the same federal laws, regulations, standards, VA directives and handbooks, as VA personnel regarding information and information system security and privacy.

B2. VA INFORMATION CUSTODIAL LANGUAGE

a. The Government shall receive unlimited rights to data/intellectual property first produced and delivered in the performance of this contract or order (hereinafter “contract”) unless expressly stated otherwise in this contract. This includes all rights to source code and all documentation created in support thereof. The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

b. Information made available to the Contractor by VA for the performance or administration of this contract will be used only for the purposes specified in the service agreement, SOW, PWS, PD, and/or contract. The Contractor shall not use VA information in any other manner without prior written approval from a VA Contracting Officer (CO). The primary clause used to define Government and Contractor data rights is FAR 52.227-14 Rights in Data – General.

c. VA information will not be co-mingled with any other data on the Contractor's information systems or media storage systems. The Contractor shall ensure compliance with Federal and VA requirements related to data protection, data encryption, physical data segregation, logical data segregation, classification requirements and media sanitization.

d. VA reserves the right to conduct scheduled or unscheduled audits, assessments, or investigations of Contractor Information Technology (IT) resources to ensure information security is compliant with Federal and VA requirements. The Contractor shall provide all necessary access to records (including electronic and documentary materials related to the contracts and subcontracts) and support (including access to Contractor and Subcontractor staff associated with the contract) to VA, VA's Office Inspector General (OIG), and/or Government Accountability Office (GAO) staff during periodic control assessments, audits, or investigations.

e. The Contractor may only use VA information within the terms of the contract and applicable Federal law, regulations, and VA policies. If new Federal information security laws, regulations or VA policies become applicable after execution of the contract, the parties agree to negotiate contract modification and adjustment necessary to implement the new laws, regulations, and/or policies.

f. The Contractor shall not make copies of VA information except as specifically authorized and necessary to perform the terms of the contract. If copies are made for restoration purposes, after the restoration is complete, the copies shall be destroyed in accordance with VA Directive 6500, VA Cybersecurity Program and VA Information Security Knowledge Service.

g. If a Veterans Health Administration (VHA) contract is terminated for default or cause with a business associate, the related local Business Associate Agreement (BAA) shall also be terminated and actions taken in accordance with VHA Directive 1605.05, Business Associate Agreements. If there is an executed national BAA associated with the contract, VA will determine what actions are appropriate and notify the contractor.

h. The Contractor shall store and transmit VA sensitive information in an encrypted form, using VA-approved encryption tools which are, at a minimum, Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules (or its successor) validated and in conformance with VA Information Security Knowledge Service requirements. The Contractor shall transmit VA sensitive information using VA approved Transport Layer Security (TLS) configured with FIPS based cipher suites in conformance with National

Institute of Standards and Technology (NIST) 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations.

i. The Contractor's firewall and web services security controls, as applicable, shall meet or exceed VA's minimum requirements.

j. Except for uses and disclosures of VA information authorized by this contract for performance of the contract, the Contractor may use and disclose VA information only in two situations: (i) in response to a qualifying order of a court of competent jurisdiction after notification to VA CO (ii) with written approval from the VA CO. The Contractor shall refer all requests for, demands for production of or inquiries about, VA information and information systems to the VA CO for response.

k. Notwithstanding the provision above, the Contractor 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 medical records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse or infection with Human Immunodeficiency Virus (HIV). If the Contractor is in receipt of a court order or other requests for the above-mentioned information, the Contractor shall immediately refer such court order or other requests to the VA CO for response.

l. Information made available to the Contractor by VA for the performance or administration of this contract or information developed by the Contractor in performance or administration of the contract will be protected and secured in accordance with VA Directive 6500 and Identity and Access Management (IAM) Security processes specified in the VA Information Security Knowledge Service.

m. Any data destruction done on behalf of VA by a Contractor shall be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management, VA Handbook 6300.1, Records Management Procedures, and applicable VA Records Control Schedules.

n. The Contractor shall provide its plan for destruction of all VA data in its possession according to VA Directive 6500 and NIST 800-88, Guidelines for Media Sanitization prior to termination or completion of this contract. If directed by the COR/CO, the Contractor shall return all Federal Records to VA for disposition.

o. Any media, such as paper, magnetic tape, magnetic disks, solid state devices or optical discs that is used to store, process, or access VA information that cannot be destroyed shall be returned to VA. The Contractor shall hold the appropriate material until otherwise directed by the Contracting Officer's Representative (COR) or CO. Items shall be returned securely via VA-approved methods. VA sensitive information must be transmitted utilizing VA-approved encryption tools which are validated under FIPS 140-2 (or its successor) and NIST 800-52. If mailed, the Contractor shall send via a trackable method (USPS, UPS, FedEx,

etc.) and immediately provide the COR/CO with the tracking information. Self-certification by the Contractor that the data destruction requirements above have been met shall be sent to the COR/CO within 30 business days of termination of the contract.

p. All electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) used to store, process or access VA information will not be returned to the Contractor at the end of lease, loan, or trade-in. Exceptions to this paragraph will only be granted with the written approval of the VA CO.

B3. 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 and subcontractors only to the extent necessary to perform the services specified in the solicitation or contract. This includes indirect entities, both affiliate of Contractor/Subcontractor and agent of Contractor/Subcontractor.

b. Contractors and subcontractors shall sign the VA Information Security Rule of Behavior (ROB) before access is provided to VA information and information systems (see Section 4, Training, below). The ROB contains the minimum user compliance requirements and does not supersede any policies of VA facilities or other agency components which provide higher levels of protection to VA's information or information systems. Users who require privileged access shall complete the VA elevated privilege access request processes before privileged access is granted.

c. All Contractors and Subcontractors working with VA information are subject to the same security investigative and clearance 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 shall be in accordance with VA Directive and Handbook 0710, Personnel Vetting Program. The Office of Human Resources and Administration/Operations, Security and Preparedness (HRA/OSP) is responsible for these policies and procedures. Contract personnel who require access to classified information or information systems shall have an appropriate security clearance. Verification of a Security Clearance shall be processed through the Special Security Officer located in HRA/OSP. Contractors shall conform to all requirements stated in the National Industrial Security Program Operating Manual (NISPOM).

d. All Contractors and subcontractors shall comply with conditions specified in VAAR 852.204-71(d); Contractor operations required to be in United States. All Contractors and Subcontractors working with VA information must be permanently located within a jurisdiction subject to the law of the United States or its Territories to the maximum extent feasible. If services are proposed to be performed abroad the Contractor must state where all non-U.S. services are provided. The Contractor shall deliver to VA a detailed plan specifically addressing communications, personnel control, data protection and potential

legal issues. The plan shall be approved by the COR/CO in writing prior to access being granted.

e. The Contractor shall notify the COR/CO in writing immediately (no later than 24 hours) after personnel separation or occurrence of other causes. Causes may include the following:
   (1) Contractor/Subcontractor personnel no longer has a need for access to VA information or VA information systems.

   (2) Contractor/Subcontractor personnel are terminated, suspended, or otherwise has their work on a VA project discontinued for any reason.

   (3) Contractor believes their own personnel or Subcontractor personnel may pose a threat to their company's working environment or to any company-owned property. This includes Contractor-owned assets, buildings, confidential data, customers, employees, networks, systems, trade secrets and/or VA data.

   (4) Any previously undisclosed changes to Contractor/Subcontractor background history are brought to light, including but not limited to changes to background investigation or employee record.

   (5) Contractor/Subcontractor personnel have their authorization to work in the United States revoked.

   (6) Agreement by which Contractor provides products and services to VA has either been fulfilled or terminated, such that VA can cut off electronic and/or physical access for Contractor personnel.

f. In such cases of contract fulfillment, termination, or other causes; the Contractor shall take the necessary measures to immediately revoke access to VA network, property, information, and information systems (logical and physical) by Contractor/Subcontractor personnel. These measures include (but are not limited to): removing and then securing Personal Identity Verification (PIV) badges and PIV – Interoperable (PIV-I) access badges, VA-issued photo badges, credentials for VA facilities and devices, VA-issued laptops, and authentication tokens. Contractors shall notify the appropriate VA COR/CO immediately to initiate access removal.

g. Contractors/Subcontractors who no longer require VA accesses will return VA-issued property to VA. This property includes (but is not limited to): documents, electronic equipment, keys, and parking passes. PIV and PIV-I access badges shall be returned to the nearest VA PIV Badge Issuance Office. Once they have had access to VA information, information systems, networks and VA property in their possessions removed, Contractors shall notify the appropriate VA COR/CO.

B4. TRAINING

a. All contractors and subcontractors requiring access to VA information and VA information systems shall successfully complete the following before being granted access to VA information and its systems:

(1) VA Privacy and Information Security Awareness and Rules of Behavior course (Talent Management System (TMS) #10176) initially and annually thereafter.

(2) Sign and acknowledge (electronically through TMS #10176) understanding of and responsibilities for compliance with the Organizational Rules of Behavior, relating to access to VA information and information systems initially and annually thereafter; and

(3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system or information access [to be defined by the VA program official and provided to the VA CO for inclusion in the solicitation document – i.e., any role-based information security training].

b. The Contractor shall provide to the COR/CO a copy of the training certificates and certification of signing the Organizational Rules of Behavior for each applicable employee within five days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training 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 required training is complete.

B5. SECURITY INCIDENT INVESTIGATION

a. The Contractor, Subcontractor, their employees, or business associates shall immediately (within one hour) report suspected security / privacy incidents to the VA OIT's Enterprise Service Desk (ESD) by calling (855) 673-4357 (TTY: 711). The ESD is OIT's 24/7/365 single point of contact for IT-related issues. After reporting to the ESD, the Contractor, Subcontractor, their employees, or business associates shall, within one hour, provide the COR/CO the incident number received from the ESD.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor's notice to VA shall identify the information involved and the circumstances surrounding the incident, including the following:

(1) The date and time (or approximation of) the Security Incident occurred.

(2) The names of individuals involved (when applicable).

(3) The physical and logical (if applicable) location of the incident.

(4) Why the Security Incident took place (i.e., catalyst for the failure).

(5) The amount of data belonging to VA believed to have been compromised.

(6) The remediation measures the Contractor is taking to ensure no future incidents of a similar nature.

c. After the Contractor has provided the initial detailed incident summary to VA, they will continue to provide written updates on any new and relevant circumstances or facts they discover. The Contractor, Subcontractor, and their employes shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

d. VA IT Contractors shall follow VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, and VA Information Security Knowledge Service guidance for implementing an Incident Response Plan or integrating with an existing VA implementation.

e. In instances of theft or 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 the VA Office of Security and Law Enforcement. The Contractor, its employees, and 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.

f. The Contractor shall comply with VA Handbook 6500.2, Management of Breaches Involving Sensitive Personal Information, which establishes the breach management policies and assigns responsibilities for the oversight, management and reporting procedures associated with managing of breaches.

g. With respect to unsecured Protected Health Information (PHI), the Contractor is deemed to have discovered a data breach when the Contractor knew or should have known of breach of such information. When a business associate is part of VHA contract, notification to the covered entity (VHA) shall be made in accordance with the executed BAA.

h. 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 involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract; the Contractor shall pay liquidated damages to the VA as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

B6. N/A

B7. INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE OR USE

a. The Contractor shall comply with all Federal laws, regulations, and VA policies for Information systems (cloud and non-cloud) that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities. Security controls for collecting, processing, transmitting, and storing of VA sensitive information, must be in place. The controls will be tested by VA or a VA sanctioned 3PAO and approved by VA prior to hosting, operation, maintenance or use of the information system or systems by or on behalf of VA. This includes conducting compliance risk assessments, security architecture analysis, routine vulnerability scanning, system patching, change management procedures and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures shall be the same as procedures used to secure VA-operated information systems.

b. Outsourcing (Contractor facility, equipment, or staff) of systems or network operations, telecommunications services or other managed services require Assessment and Authorization (A&A) of the Contractor's systems in accordance with VA Handbook 6500 as specified in VA Information Security Knowledge Service. Major changes to the A&A package may require reviewing and updating all the documentation associated with the change. The Contractor's cloud computing systems shall comply with FedRAMP and VA Directive 6517 requirements.

c. The Contractor shall return all electronic storage media (hard drives, optical disks, CDs, back-up tapes, etc.) on non-VA leased or non-VA owned IT equipment used to store, process or access VA information to VA in accordance with A&A package requirements. This applies when the contract is terminated or completed and prior to disposal of media. The Contractor shall provide its plan for destruction of all VA data in its possession according to VA Information Security Knowledge Service requirements and NIST 800-88. The Contractor shall send a self-certification that the data destruction requirements above have been met to the COR/CO within 30 business days of termination of the contract.

d. All external internet connections to VA network involving VA information must be in accordance with VA Trusted Internet Connection (TIC) Reference Architecture and VA Directive and Handbook 6513, Secure External Connections and reviewed and approved by VA prior to implementation. Government-owned Contractor-operated systems, third party or business partner networks require a Memorandum of Understanding (MOU) and Interconnection Security Agreements (ISA).

e. Contractor procedures shall be subject to periodic, announced, or unannounced assessments by VA officials, the OIG or a 3PAO. The physical security aspects associated with Contractor activities are also subject to such assessments. The Contractor shall report, in writing, any deficiencies noted during the above

assessment to the VA COR/CO. The Contractor shall use VA's defined processes to document planned remedial actions that address identified deficiencies in information security policies, procedures, and practices. The Contractor shall correct security deficiencies within the timeframes specified in the VA Information Security Knowledge Service.

f. All major information system changes which occur in the production environment shall be reviewed by the VA to determine the impact on privacy and security of the system. Based on the review results, updates to the Authority to Operate (ATO) documentation and parameters may be required to remain in compliance with VA Handbook 6500 and VA Information Security Knowledge Service requirements.

g. The Contractor shall conduct an annual privacy and security self-assessment on all information systems and outsourced services as required. Copies of the assessment shall be provided to the COR/CO. The VA/Government reserves the right to conduct assessment using government personnel or a third-party if deemed necessary. The Contractor shall correct or mitigate any weaknesses discovered during the assessment.

h. VA prohibits the installation and use of personally owned or Contractor-owned equipment or software on VA information systems. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW, PWS, PD or contract. All security controls required for government furnished equipment must be utilized in VA approved Other Equipment (OE). Configuration changes to the Contractor OE, must be funded by the owner of the equipment. All remote systems must use a VA-approved antivirus software and a personal (host-based or enclave based) firewall with a VA-approved configuration. The Contractor shall ensure software on OE is kept current with all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-virus software and the firewall on the non-VA owned OE. Approved Contractor OE will be subject to technical inspection at any time.

i. The Contractor shall notify the COR/CO within one hour of disclosure or successful exploits of any vulnerability which can compromise the confidentiality, integrity, or availability of the information systems. The system or effected component(s) need(s) to be isolated from the network. A forensic analysis needs to be conducted jointly with VA. Such issues will be remediated as quickly as practicable, but in no event longer than the timeframe specified by VA Information Security Knowledge Service. If sensitive personal information is compromised reference VA Handbook 6500.2 and Section 5, Security Incident Investigation.

j. For cases wherein the Contractor discovers material defects or vulnerabilities impacting products and services they provide to VA, the Contractor shall develop and implement policies and procedures for disclosure to VA, as well as remediation. The Contractor shall, within 30 business days of discovery, document a summary of these vulnerabilities or defects. The documentation will

include a description of the potential impact of each vulnerability and material defect, compensating security controls, mitigations, recommended corrective actions, root cause analysis and/or workarounds (i.e., monitoring). Should there exist any backdoors in the products or services they provide to VA (referring to methods for bypassing computer authentication), the Contractor shall provide the VA CO/CO written assurance they have permanently remediated these backdoors.

k. All other vulnerabilities, including those discovered through routine scans or other assessments, will be remediated based on risk, in accordance with the remediation timelines specified by the VA Information Security Knowledge Service and/or the applicable timeframe mandated by Cybersecurity & Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01 and BOD 19-02 for Internet-accessible systems. Exceptions to this paragraph will only be granted with the approval of the COR/CO.

B8. SECURITY AND PRIVACY CONTROLS COMPLIANCE TESTING, ASSESSMENT AND AUDITING

a. Should VA request it, the Contractor shall provide a copy of their (corporation's, sole proprietorship's, partnership's, limited liability company (LLC), or other business structure entity's) policies, procedures, evidence and independent report summaries related to specified cybersecurity frameworks (International Organization for Standardization (ISO), NIST Cybersecurity Framework (CSF), etc.). VA or its third-party/partner designee (if applicable) are further entitled to perform their own audits and security/penetration tests of the Contractor's IT or systems and controls, to ascertain whether the Contractor is complying with the information security, network or system requirements mandated in the agreement between VA and the Contractor.

b. Any audits or tests of the Contractor or third-party designees/partner VA elects to carry out will commence within 30 business days of VA notification. Such audits, tests and assessments may include the following: (a): security/penetration tests which both sides agree will not unduly impact Contractor operations; (b): interviews with pertinent stakeholders and practitioners; (c): document review; and (d): technical inspections of networks and systems the Contractor uses to destroy, maintain, receive, retain, or use VA information.

c. As part of these audits, tests and assessments, the Contractor shall provide all information requested by VA. This information includes, but is not limited to, the following: equipment lists, network or infrastructure diagrams, relevant policy documents, system logs or details on information systems accessing, transporting, or processing VA data.

d. The Contractor and at its own expense, shall comply with any recommendations resulting from VA audits, inspections and tests. VA further retains the right to view any related security reports the Contractor has generated as part of its own security assessment. The Contractor shall also notify VA of the existence of any

such security reports or other related assessments, upon completion and validation.

e. VA appointed auditors or other government agency partners may be granted access to such documentation on a need-to-know basis and coordinated through the COR/CO. The Contractor shall comply with recommendations which result from these regulatory assessments on the part of VA regulators and associated government agency partners.

B9. PRODUCT INTEGRITY, AUTHENTICITY, PROVENANCE, ANTI-COUNTERFEIT AND ANTI-TAMPERING

a. The Contractor shall comply with Code of Federal Regulations (CFR) Title 15 Part 7, “Securing the Information and Communications Technology and Services (ICTS) Supply Chain”, which prohibits ICTS Transactions from foreign adversaries. ICTS Transactions are defined as any acquisition, importation, transfer, installation, dealing in or use of any information and communications technology or service, including ongoing activities, such as managed services, data transmission, software updates, repairs or the platforming or data hosting of applications for consumer download.

b. When contracting terms require the Contractor to procure equipment, the Contractor shall purchase or acquire the equipment from an Original Equipment Manufacturer (OEM) or an authorized reseller of the OEM. The Contractor shall attest that equipment procured from an OEM or authorized reseller or distributor are authentic. If procurement is unavailable from an OEM or authorized reseller, the Contractor shall submit in writing, details of the circumstances prohibiting this from happening and procure a product waiver from the VA COR/CO.

c. All Contractors shall establish, implement, and provide documentation for risk management practices for supply chain delivery of hardware, software (to include patches) and firmware provided under this agreement. Documentation will include chain of custody practices, inventory management program, information protection practices, integrity management program for sub-supplier provided components, and replacement parts requests. The Contractor shall make spare parts available. All Contractor(s) shall specify how digital delivery for procured products, including patches, will be validated and monitored to ensure consistent delivery. The Contractor shall apply encryption technology to protect procured products throughout the delivery process.

d. If a Contractor provides software or patches to VA, the Contractor shall publish or provide a hash conforming to the FIPS Security Requirements for Cryptographic Modules (FIPS 140-2 or successor).

e. The Contractor shall provide a software bill of materials (SBOM) for procured (to include licensed products) and consist of a list of components and associated metadata which make up the product. SBOMs must be generated in one of the data formats defined in the National Telecommunications and Information

Administration (NTIA) report “The Minimum Elements for a Software Bill of Materials (SBOM).”

f. Contractors shall use or arrange for the use of trusted channels to ship procured products, such as U.S. registered mail and/or tamper-evident packaging for physical deliveries.

g. Throughout the delivery process, the Contractor shall demonstrate a capability for detecting unauthorized access (tampering).

h. The Contractor shall demonstrate chain-of-custody documentation for procured products and require tamper-evident packaging for the delivery of this hardware.

B10. VIRUSES, FIRMWARE, AND MALWARE

a. The Contractor shall execute due diligence to ensure all provided software and patches, including third-party patches, are free of viruses and/or malware before releasing them to or installing them on VA information systems.

b. The Contractor warrants it has no knowledge of and did not insert, any malicious virus and/or malware code into any software or patches provided to VA which could potentially harm or disrupt VA information systems. The Contractor shall use due diligence, if supplying third-party software or patches, to ensure the third-party has not inserted any malicious code and/or virus which could damage or disrupt VA information systems.

c. The Contractor shall provide or arrange for the provision of technical justification as to why any “false positive” hit has taken place to ensure their code’s supply chain has not been compromised. Justification may be required, but is not limited to, when install files, scripts, firmware, or other Contractor-delivered software solutions (including third-party install files, scripts, firmware, or other software) are flagged as malicious, infected, or suspicious by an anti-virus vendor.

d. The Contractor shall not upload (intentionally or negligently) any virus, worm, malware or any harmful or malicious content, component and/or corrupted data/source code (hereinafter “virus or other malware”) onto VA computer and information systems and/or networks. If introduced (and this clause is violated), upon written request from the VA CO, the Contractor shall:

    (1) Take all necessary action to correct the incident, to include any and all assistance to VA to eliminate the virus or other malware throughout VA’s information networks, computer systems and information systems; and
    (2) Use commercially reasonable efforts to restore operational efficiency and remediate damages due to data loss or data integrity damage, if the virus or other malware causes a loss of operational efficiency, data loss, or damage to data integrity.

B11. CRYPTOGRAPHIC REQUIREMENT

a. The Contractor shall document how the cryptographic system supporting the Contractor's products and/or services protect the confidentiality, data integrity, authentication and non-repudiation of devices and data flows in the underlying system.

b. The Contractor shall use only approved cryptographic methods as defined in FIPS 140-2 (or its successor) and NIST 800-52 standards when enabling encryption on its products.

c. The Contractor shall provide or arrange for the provision of an automated remote key-establishment method which protects the confidentiality and integrity of the cryptographic keys.

d. The Contractor shall ensure emergency re-keying of all devices can be remotely performed within 30 business days.

e. The Contractor shall provide or arrange for the provision of a method for updating cryptographic primitives or algorithms.

B12. PATCHING GOVERNANCE

a. The Contractor shall provide documentation detailing the patch management, vulnerability management, mitigation and update processes (to include third-party) prior to the connection of electronic devices, assets or equipment to VA's assets. This documentation will include information regarding the following:

    (1) The resources and technical capabilities to sustain the program or process (e.g., how the integrity of a patch is validated by VA); and.

    (2) The approach and capability to remediate newly reported zero-day vulnerabilities for Contractor products.

b. The Contractor shall verify and provide documentation all procured products (including third-party applications, hardware, software, operating systems, and firmware) have appropriate updates and patches installed prior to delivery to VA.

c. The Contractor shall provide or arrange the provision of appropriate software and firmware updates to remediate newly discovered vulnerabilities or weaknesses for their products and services within 30 days of discovery. Updates to remediate critical or emergent vulnerabilities will be provided within seven business days of discovery. If updates cannot be made available by Contractor within these time periods, the Contractor shall submit mitigations, methods of exploit detection and/or workarounds to the COR/CO prior to the above deadlines.

d. The Contractor shall provide or arrange for the provision of appropriate hardware, software and/or firmware updates, when those products, including open-source software, are provided to the VA, to remediate newly discovered vulnerabilities or weaknesses. Remediations of products or services provided to

the VA's system environment must be provided within 30 business days of availability from the original supplier and/or patching source. Updates to remediate critical vulnerabilities applicable to the Contractor's use of the third-party product in its system environment will be provided within seven business days of availability from the original supplier and/or patching source. If applicable third-party updates cannot be integrated, tested and made available by Contractor within these time periods, mitigations and/or workarounds will be provided to the COR/CO before the above deadlines.

B13. N/A

B14. DATA CENTER PROVISIONS

a. The Contractor shall ensure the VA network is accessed by in accordance with VA Directive 6500 and IAM security processes specified in the VA Information Security Knowledge Service.

b. The Contractor shall ensure network infrastructure and data availability in accordance with VA information system business continuity procedures specified in the VA Information Security Knowledge Service.

c. The Contractor shall ensure any connections to the internet or other external networks for information systems occur through managed interfaces utilizing VA approved boundary protection devices (e.g., internet proxies, gateways, routers, firewalls, guards or encrypted tunnels).

d. The Contractor shall encrypt all traffic across the segment of the Wide Area Network (WAN) it manages and no unencrypted Out of Band (OOB) Internet Protocol (IP) traffic will traverse the network.

e. The Contractor shall ensure tunnel endpoints are routable addresses at each VA operating site.

f. The Contractor shall secure access from Local Area Networks (LANs) at co-located sites in accordance with VA TIC Reference Architecture, VA Directive and Handbook 6513, and MOU/ISA process specified in the VA Information Security Knowledge Service.

SECTION C - CONTRACT CLAUSES

C.1 ADDENDUM to RFO 52.212-4 TERMS AND CONDITIONS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES

The following clauses are incorporated into 52.212-4 as an addendum to this contract:

C.2 RFO FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

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 this/these address(es):

RFO/FAR: https://www.acquisition.gov/far-overhaul
VAAR: https://www.acquisition.gov/vaar

RFO Number	Title	Date
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT (ALTERNATIVE I)	JUN 2020
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	NOV 2021
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS	NOV 2023
52.203-19	PROHIBITION ON CERTAIN CONFIDENTIALITY AGREEMENTS	JAN 2017
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	JAN 2011
52.204-13	SYSTEM FOR AWARD MANAGEMENT-MAINTENANCE	DEV NOV 2025
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, PROPOSED FOR DEBARMENT, OR VOLUNTARILY EXCLUDED	DEV NOV 2025
52.209-9	UPDATES OF PUBLICLY AVAILABLE INFORMATION REGARDING RESPONSIBILITY MATTERS	DEV NOV 2025
52.209-10	INVERTED DOMESTIC CORPORATIONS	DEV NOV 2025

52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	DEV NOV 2025
52.219-9	SMALL BUSINESS SUBCONTRACTING PLAN	DEV NOV 2025
52.219-16	LIQUIDATED DAMAGES-SUBCONTRACTING PLAN	DEV NOV 2025
52.222-3	CONVICT LABOR	DEV NOV 2025
52.222-19	CHILD LABOR	DEV NOV 2025
52.222-35	EQUAL OPPORTUNITY FOR VETERANS	DEV NOV 2025
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES	DEV NOV 2025
52.222-37	EMPLOYMENT REPORTS ON VETERANS	DEV NOV 2025
52.222-40	EMPLOYEE RIGHTS UNDER NLRA	DEV NOV 2025
52.222-50	COMBATTING TRAFFICKING IN PERSONS	DEV NOV 2025
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	DEV NOV 2025
52.226-8	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING	MAY 2024
52.227-14	RIGHTS IN DATA-GENERAL	MAY 2014
52.232-33	PAYMENT BY ELECTRONIC FUNDS TRANSFER-SYSTEM FOR AWARD MANAGEMENT	OCT 2018
52.232-40	ACCELERATED PAYMENTS TO SMALL BUSINESS SUBS	MAR 2023

52.233-3	PROTEST AFTER AWARD	DEV NOV 2025
52.233-4	APPLICABLE LAW FOR BREACH	DEV NOV 2025
52.227-1	AUTHORIZATION AND CONSENT	JUN 2020
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	JUN 2020
52.240-91	SECURITY PROHIBITIONS AND EXCLUSIONS	DEV NOV 2025
52.204-21	BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS	DEV NOV 2025
52.244-6	SUBCONTRACTS FOR COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	DEV NOV 2025
852.201-70	CONTRACTING OFFICERS REPRESENTATIVE	DEC 2022
852.203-70	COMMERCIAL ADVERTISING	MAY 2018
852.219-70	VA SMALL BUSINESS SUBCONTRACTING PLAN MINIMUM REQUIREMENTS	DEV JAN 2023
852.232-72	ELECTRONIC SUBMISSION OF PAYMENT REQUESTS	NOV 2018
852.239-70	SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES	FEB 2023
852.239-71	INFORMATION SYSTEM SECURITY PLAN AND ACCREDITATION	FEB 2023
852.239-76	INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY	FEB 2023
852.242-71	ADMINISTRATIVE CONTRACTING OFFICER	OCT 2020

(End of Clause)

C.3 RFO 52.216-18 ORDERING (AUG 2020)

(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 date of award to 5 years or 60 months after award (specific dates to be determined at award).

(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.

(End of clause)

C.4 RFO 52.216-19 ORDERING LIMITATIONS (OCT 1995)

(a) Minimum order. When the Government requires supplies or services covered by this contract in an amount of less than $280.00, 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 $50,000,000.00;

(2) Any order for a combination of items in excess of $50,000,000.00; or

(3) A series of orders from the same ordering office within 30 days that together call for quantities exceeding the limitation in paragraph (b)(1) or (2) of this section.

(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) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, 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 __7___ 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)

C.5 RFO 52.216-22 INDEFINITE QUANTITY (NOV 2025)

(a) This is an indefinite-quantity, indefinite-delivery contract for the supplies or services specified, and effective for the period stated, in the Schedule.

(b) The Government shall order the quantity of supplies or services specified in the Schedule, and the Contractor shall furnish them when ordered. Delivery or performance shall be at locations designated in orders issued in accordance with the Ordering clause and the Schedule.

(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 ordering period of this contract and not completed within that time shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after one year or 12 months after contract expiration.

(End of clause)

C.6 VAAR 852.204-70 PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL (MAY 2020)

(a) The Contractor shall comply with current Department of Veterans Affairs policy for personal identity verification of all employees performing under this contract when frequent and continuing access to VA facilities or information systems is required.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor's employees will require frequent and continuing access to VA facilities or information systems.

(End of clause)

C.7 VAAR 852.204-71 INFORMATION AND INFORMATION SYSTEMS SECURITY (MAR 2026)

(a) Definitions. As used in this clause—

Business Associate means an entity, including an individual (other than a member of the workforce of a covered entity), company, organization or another covered entity, as defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule, that performs or assists in the performance of a function or activity on

behalf of the Veterans Health Administration (VHA) that involves the creating, receiving, maintaining, transmitting of, or having access to, protected health information (PHI). The term also includes a subcontractor of a business associate that creates, receives, maintains, or transmits PHI on behalf of the business associate.

Business Associate Agreement (BAA) means the agreement, as dictated by the Privacy Rule, between VHA and a business associate, which must be entered into in addition to the underlying contract for services and before any release of PHI can be made to the business associate, in order for the business associate to perform certain functions or activities on behalf of VHA.

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.

Information technology (see FAR 2.101) also means Information and Communication Technology (ICT).

Information technology-related contracts means those contracts which include services (including support services), and related resources for information technology as defined in 802.101.

Privacy officer means the VA official with responsibility for implementing and oversight of privacy related policies and practices that impact a given VA acquisition.

Sensitive personal information means, with respect to an individual, any information about the individual maintained by VA, including but not limited to the following:

(1) Education, financial transactions, medical history, and criminal or employment history.

(2) Information that can be used to distinguish or trace the individual's identity, including but not limited to name, social security number, date and place of birth, mother's maiden name, or biometric records.

Security plan means a formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements.

VA Information Security Rules of Behavior for Organizational Users (VA National Rules of Behavior) means a set of VA rules that describes the responsibilities and expected behavior of users of VA information or information systems.

VA sensitive information means all VA data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes sensitive personal information. The term includes information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and

personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs

(b) General. Contractors, subcontractors, their employees, third-parties, and business associates with access to VA information, information systems, or information technology (IT) or providing and accessing IT-related goods and services, shall adhere to VA Directive 6500, VA Cybersecurity Program, and the directives and handbooks in the VA 6500 series related to VA information (including VA sensitive information and sensitive personal information and information systems security and privacy), as well as those set forth in the contract specifications, statement of work, or performance work statement. These include, but are not limited to, VA Handbook 6500.6, Contract Security; and VA Directive and Handbook 0710, Personnel Security and Suitability Program, which establishes VA's procedures, responsibilities, and processes for complying with current Federal law, Executive Orders, policies, regulations, standards and guidance for protecting VA information, information systems (see 802.101, Definitions) security and privacy, and adhering to personnel security requirements when accessing VA information or information systems.

(c) Access to VA information and VA information systems. (1) Contractors are limited in their request for logical or physical access to VA information or VA information systems for their employees, subcontractors, third parties and business associates to the extent necessary to perform the services or provide the goods as specified in the contracts, agreements, task, delivery or purchase orders.

(2) All Contractors, subcontractors, third parties, and business 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 to access VA information and VA information systems shall be in accordance with VA Directive and Handbook 0710, Personnel Security and Suitability Program.

(3) Contractors, subcontractors, third parties, and business associates who require access to national security programs must have a valid security clearance.

(4) HIPAA Business Associate Agreement requirement. Contractors shall enter into a Business Associate Agreement (BAA) with VHA, VA's Covered Entity, when contract requirements and access to protected health information is required and when requested by the Contracting Officer, or the Contracting Officer's Representative (COR) (see VAAR 824.103-70). Under the HIPAA Privacy and Security Rules, a Covered Entity (VHA) must have a satisfactory assurance that its PHI will be safeguarded from misuse. To do so, a Covered Entity enters into a BAA with a contractor (now the business associate), which obligates the business associate to only use the Covered Entity's PHI for the purposes for which it was engaged, provide the same protections and safeguards as is required from the Covered Entity, and agree to the same

disclosure restrictions to PHI that is required of the Covered Entity in situations where a contractor—

(i) Creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain health care operations activities or functions on behalf of the Covered Entity; or

(ii) Provides one or more of the services specified in the Privacy Rule to or for the Covered Entity.

(A) Contractors or entities required to execute BAAs for contracts and other agreements become VHA business associates. BAAs are issued by VHA or may be issued by other VA programs in support of VHA. The HIPAA Privacy Rule requires VHA to execute compliant BAAs with persons or entities that create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI in order to perform certain activities, functions or services to, for, or on behalf of VHA. There may be other VA components or staff offices which also provide certain services and support to VHA and must receive PHI in order to do so. If these components award contracts or enter into other agreements, purchase/delivery orders, modifications and issue governmentwide purchase card transactions to help in the delivery of these services to VHA, they will also fall within the requirement to obtain a satisfactory assurance from these contractors by executing a BAA.

(B) BAA requirement flow down to subcontractors. A prime Contractor required to execute a BAA shall also obtain a satisfactory assurance, in the form of a BAA, that any of its subcontractors who will also create, receive, maintain, or transmit VHA PHI or that will store, generate, access, exchange, process, or utilize such PHI will comply with HIPAA requirements to the same degree as the Contractor. Contractors employing a subcontractor who creates, receives, maintains, or transmits VHA PHI or that will store, generate, access, exchange, process, or utilize such VHA PHI under a contract or agreement is required to execute a BAA with each of its subcontractors which also obligates the subcontractor (i.e., also a business associate) to provide the same protections and safeguards and agree to the same disclosure restrictions to VHA’s PHI that is required of the Covered Entity and the prime Contractor.

(d) Contractor operations required to be in United States. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practicable. If such services are proposed to be performed outside the continental United States, and are not otherwise disallowed by other Federal law, regulations or policy, or other VA policy or other mandates as stated in the contract, specifications, statement of work or performance work statement (including applicable Business Associate Agreements), the Contractor/subcontractor must state in its proposal where all non-U.S. services are provided. At a minimum, the Contractor/subcontractor must include a detailed Information Technology Security Plan, for review and approval by the Contracting Officer, specifically to address mitigation of the resulting problems of communication, control, and data protection.

(e) Contractor/subcontractor employee reassignment and termination notification. Contractors and subcontractors shall provide written notification to the Contracting Officer and Contracting Officer’s Representative (COR) immediately, and not later than four (4) hours, when an employee working on a VA information system or with access to

VA information is reassigned or leaves the Contractor or subcontractor's employment on the cognizant VA contract. The Contracting Officer and COR must also be notified immediately by the Contractor or subcontractor prior to an unfriendly termination.

(f) VA information custodial requirements. (1) Release, publication, and use of data. Information made available to a Contractor or subcontractor by VA for the performance or administration of a contract or information developed by the Contractor/subcontractor in performance or administration of a contract shall be used only for the stated contract purpose and shall not be used in any other way without VA's prior written approval. This clause expressly limits the Contractor's/subcontractor's rights to use data as described in Rights in Data—General, FAR 52.227-14(d).

(2) Media sanitization. VA information shall not be co-mingled with any other data on the Contractors/subcontractor's information systems or media storage systems in order to ensure federal and VA requirements related to data protection, information segregation, classification requirements, and media sanitization can be met (see VA Directive 6500, VA Cybersecurity Program).VA reserves the right to conduct scheduled or unscheduled on-site inspections, assessments, or audits of Contractor and subcontractor IT resources, information systems and assets to ensure data security and privacy controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with Federal and VA requirements. The Contractor and subcontractor will provide all necessary access and support to VA and/or GAO staff during periodic control assessments or audits.

(3) Data retention, destruction, and contractor self-certification. The Contactor and its subcontractors are responsible for collecting and destroying any VA data provided, created, or stored under the terms of this contract, to a point where VA data or materials are no longer readable or reconstructable to any degree, in accordance with VA Directive 6371, Destruction of Temporary Paper Records, or subsequent issue. Prior to termination or completion of this contract, the Contractor/subcontractor must provide its plan for destruction of all VA data in its possession according to VA Directive 6500, and VA Cybersecurity Program, including compliance with National Institute of Standards and Technology (NIST) 800-88, Guidelines for Media Sanitization, for the purposes of media sanitization on all IT equipment. The Contractor must certify in writing to the Contracting Officer within 30 days of termination of the contract that the data destruction requirements in this paragraph have been met.

(4) Return of VA data and information. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to the VA (as stipulated by the Contracting Officer or the COR) or the Contractor/subcontractor must hold it until otherwise directed. Items returned will be hand carried, securely mailed, emailed, or securely electronically transmitted to the Contracting Officer or to the address as provided in the contract or by the assigned COR, and/or accompanying BAA. Depending on the method of return, Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract using VA-approved encryption tools that are, at a minimum, validated under Federal Information Processing Standards (FIPS) 140-3 (or its successor). If mailed, Contractor/subcontractor must send via a trackable method (USPS, UPS, Federal Express, etc.) and immediately provide the Contracting Officer with the tracking information.No information, data, documentary material, records or equipment will be

destroyed unless done in accordance with the terms of this contract and the VHA Records Control Schedule 10-1.

(5) Use of VA data and information. 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 the National 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 for this contract as a result of any updates, if required.

(6) Copying VA data or information. The Contractor/subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the contract 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, after the restoration is complete, the copies must be appropriately destroyed.

(7) Violation of information custodial requirements. If VA determines that the Contractor has violated any of VA’s information confidentiality, privacy, or security provisions, it shall be sufficient grounds for VA to withhold payment to the Contractor or third-party or terminate the contract for default in accordance with FAR part 49 or terminate for cause in accordance with FAR 12.403.

(8) Encryption. The Contractor/subcontractor must store, transport, or transmit VA sensitive information, when permitted by the contract, using cryptography, and VA-approved encryption tools that are, at a minimum, validated under FIPS 140-3 (or its successor).

(9) Firewall and web services security controls. 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.

(10) Disclosure of VA data and information. Except for uses and disclosures of VA information authorized in a cognizant contract for performance of the contract, the Contractor/subcontractor may use and disclose VA information only in two other situations: (i) subject to paragraph (f)(10) of this section, in response to a court order from 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 Contracting Officer for response. If the Contractor/subcontractor is in receipt of a court order or other request or believes it has a legal requirement to disclose VA information, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response. If the Contractor or subcontractor discloses information on behalf of VHA, the Contractor and/or subcontractor must maintain an accounting of disclosures. Accounting of Disclosures documentation maintained by the Contractor/subcontractor will include the name of the individual to whom the information

pertains, the date of each disclosure, the nature or description of the information disclosed, a brief statement of the purpose of each disclosure or, in lieu of such statement, a copy of a written request for a disclosure, and the name and address of the person or agency to whom the disclosure was made. The Contractor/subcontractor will provide its Accounting of Disclosures upon request and within 15 calendar days to the assigned COR and Privacy Officer. Accounting of disclosures should be provided electronically via encrypted email to the COR and designated VA facility Privacy Officer as provided in the contract, BAA, or by the Contracting Officer. If providing the Accounting of Disclosures electronically cannot be done securely, the Contractor/subcontractor will provide copies via trackable methods (UPS, USPS, Federal Express, etc.) immediately, providing the designated COR and Privacy Officer with the tracking information.

(11) Compliance with privacy statutes and applicable regulations. The Contractor/subcontractor shall not disclose VA information protected by any of VA's privacy statutes or applicable regulations including but not limited to: the Privacy Act of 1974, 38 U.S.C. 5701, confidential nature of claims, 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or 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 or the HIPAA Privacy Rule. If the Contractor/subcontractor is in receipt of a court order or other requests for VA information or has questions if it can disclose information protected under the above-mentioned confidentiality statutes because it is required by law, that Contractor/subcontractor shall immediately refer such court order or other request to the Contracting Officer for response.

(g) Report of known or suspected security/privacy incident. The Contractor, subcontractor, third-party affiliate or business associate, and its employees shall notify VA immediately via the Contracting Officer and the COR or within one (1) hour of an incident which is an occurrence (including the discovery or disclosure of successful exploits of system vulnerability) that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or the availability of its data and operations, or of its information or information system(s); or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. The initial notification may first be made verbally but must be followed up in writing within one (1) hour. See VA Data Breach Response Service at https://www.oprm.va.gov/dbrs/about_dbrs.aspx. Report all actual or suspected security/privacy incidents and report the information to the Contracting Officer and the COR as identified in the contract or as directed in the contract, within one hour of discovery or suspicion.

(1) Such issues shall be remediated as quickly as is practical, but in no event longer than 30 days. The Contractor shall notify the Contracting Officer in writing.

(2) When the security fixes involve installing third party patched (e.g., Microsoft OS patches or Adobe Acrobat), the Contractor will provide written notice to VA that the patch has been validated as not affecting the systems within 10 working days. When the Contractor is responsible for operations or maintenance of the systems, they shall apply the security fixes within 10 business days.

(3) All other vulnerabilities shall be remediated in a timely manner based on risk, but within 60 days of discovery or disclosure. Contractors shall notify the Contracting Officer, and COR within 2 business days after remediation of the identified vulnerability. Exceptions to this paragraph (e.g., for the convenience of VA) must be requested by the Contractor through the COR and shall only be granted with approval of the Contracting Officer and the VA Assistant Secretary for Office of Information and Technology. These exceptions will be tracked by the Contractor in concert with the Government in accordance with VA Directive 6500 and related VA Handbooks.

(h) Security and privacy incident investigation. (1) The term “privacy incident” means the unauthorized disclosure or use of VA information protected under a confidentiality statute or regulation.

(2) The term "security incident" means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information systems; or (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable policies. The Contractor/ subcontractor shall immediately notify the Contracting Officer and COR for the contract of any known or suspected security or privacy incident, or any other unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/subcontractor has access.

(3) 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.

(4) With respect to unsecured PHI, the Business Associate is deemed to have discovered a security incident as defined above when the Business Associate either knew, or by exercising reasonable diligence should have been known to an employee of the Business Associate. Upon discovery, the Business Associate must notify VHA of the security incident immediately within one hour of discovery or suspicion as agreed to in the BAA.

(5) In instances of theft or 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 the VA Office of Security and Law Enforcement. The Contractor, its employees, and 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.

(i) Data breach notification requirements. (1) This contract may require access to sensitive personal information. If so, the Contractor is liable to VA for liquidated damages in the event of a data breach involving any VA sensitive personal information the Contractor/Subcontractor processes or maintains under the contract as set forth in clause 852.211-76, Liquidated Damages—Reimbursement for Data Breach Costs.

(2) The Contractor/subcontractor shall provide notice to VA of a privacy or security incident as set forth in the Security and Privacy Incident Investigation section of this clause. The term 'data breach' means the loss, theft, or other unauthorized access, or any access other than that incidental to the scope of employment, to data containing sensitive personal information, in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data. The Contractor shall fully cooperate with VA or third-party entity performing an independent risk analysis on behalf of VA. Failure to cooperate may be deemed a material breach and grounds for contract termination.

(3) The Contractor/subcontractor shall fully cooperate with VA or any Government agency conducting an analysis regarding any notice of a data breach or potential data breach or security incident which may require the Contractor to provide information to the Government or third-party performing a risk analysis for VA, and shall address all relevant information concerning the data breach, including the following:

(i) Nature of the event (loss, theft, unauthorized access).

(ii) Description of the event, including—

(A) Date of occurrence;

(B) Date of incident detection;

(C) Data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code.

(D) Number of individuals affected or potentially affected.

(E) Names of individuals or groups affected or potentially affected.

(F) Ease of logical data access to the lost, stolen or improperly accessed data in light of the degree of protection for the data, e.g., unencrypted, plain text.

(G) Amount of time the data has been out of VA control.

(H) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons).

(I) Known misuses of data containing sensitive personal information, if any.

(J) Assessment of the potential harm to the affected individuals.

(K) Data breach analysis as outlined in 6500.2 Handbook, Management of Breaches Involving Sensitive Personal Information, as appropriate.

(L) Whether credit protection services may assist record subjects in avoiding or mitigating the results of identity theft based on the sensitive personal information that may have been compromised.

(M) Steps taken in response to mitigate or prevent a repetition of the incident.

(j) Training. (1) All Contractor employees and subcontractor employees requiring access to VA information or VA information systems shall complete the following before being granted access to VA information and its systems:

(i) On an annual basis, successfully complete the VA Privacy and Information Security Awareness and VA Information Security Rules of Behavior training.

(ii) On an annual basis, sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the VA Information Security Rules of Behavior for Organizational Users, relating to access to VA information and information systems.

(iii) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access.

(2) The Contractor shall provide to the Contracting Officer and/or the COR a copy of the training certificates and affirmation that VA Information Security Rules of Behavior for Organizational Users signed by each applicable employee have been completed and submitted within five (5) days of the initiation of the contract and annually thereafter, as required.

(3) Failure to complete the mandatory annual training and acknowledgement of the VA Information Security Rules of Behavior, 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.

(k) Subcontract flow down. The Contractor shall include the substance of this clause, including this paragraph (k), in subcontracts, third-party agreements, and BAAs, of any amount and in which subcontractor employees, third-party servicers/employees, and business associates will perform functions where they will have access to VA information (including VA sensitive information, i.e., sensitive personal information and protected health information), information systems, information technology (IT) or providing and accessing information technology-related contract services, support services, and related resources (see VAAR 802.101 definition of information technology-related contracts).

(End of clause)

C.8 852.204-72 PERSONNEL VETTING AND CREDENTIALING (MAR 2026)

a. Definitions. As used in this clause –

VA Information system is the same as information system and means, pursuant to 38 U.S.C. 5727, a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information whether automated or manual.

VA sensitive information means all VA data, on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information and includes sensitive personal information. The term includes information where improper use or disclosure could adversely affect the ability of VA to accomplish its mission, proprietary information, records about individuals requiring protection under various

confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of Federal programs.

b. General. Contractor personnel assigned to work for or on behalf of VA must undergo a background investigation commensurate with the risk and sensitivity level designation associated with the work to be performed at the level indicated in the contract. The Contractor and subcontractors shall comply with VA Directive/Handbook 0710, Personnel Security and Suitability Program, which can be accessed at: https://vaww.va.gov/vapubs/index.cfm

c. Risk and Sensitivity Levels. The following table identifies the risk and sensitivity levels that apply to any personnel providing services under this contract. *VA Administrations, organizations and staff offices will use the OPM Position Designation Tool.

Positions/Tasks Designated as Non-Sensitive Positions - Tier 1/Low Risk
Product Description Section 6.1
Positions/Tasks Designated as Non-Sensitive Positions- Tier 2/Mod Risk
NA
Positions/Tasks Designated as Non-Sensitive Positions - Tier 4/High Risk
NA

Security clearances are granted to individuals with a specific requirement for access to classified material (for example, Confidential, Secret and Top Secret). Contractor personnel that are required to obtain a security clearance will be subject to a Tier 3 or Tier 5 investigation. The following sensitivity designations have been assigned for the identified Tier 3 and Tier 5 required by this contract:

Tier 3: Not Applicable

Tier 5: Not Applicable

d. Fitness. The results from a background investigation are used to determine if an individual's fitness is sufficient for that individual to perform work for or on behalf of VA in the position identified in this contract. Contractor fitness determinations are made in accordance with 5 CFR Part 731.202.

Fitness requirements for employment are separate and distinct from job qualifications. If a Contractor or subcontractor employee is found to be unsuitable or unfit to provide services under this contract, the Contractor shall immediately remove the employee from working on this contract and take those necessary steps that restrict the

employee's logical access to VA data, information, VA sensitive information, or information technology or VA information systems containing such data or information.

The Contractor shall advise the employee that they are not permitted to access any VA controlled building or real property in relation to this contract.
The removal of an unfit Contractor or subcontractor employee does not alleviate the Contractor from satisfying the requirements of this contract. The Government will not reimburse the Contractor for any costs associated with the recruitment/replacement of an employee or subcontractor employee who is found to be unfit.

e. Identification Cards. The Government will provide a Personal Identification Verification (PIV) card or other identification card, as necessary, to fit Contractor personnel who require physical access to VA facilities and/or logical access to VA data, information, VA sensitive information, or information technology or VA information systems containing such data or information. Contractor and subcontractor personnel shall prominently display their PIV/identification card on their persons while working at a VA facility and shall present their PIV/identification card for inspection upon request by a VA official. The Contractor must surrender the employee or subcontractor employee's PIV/identification card in accordance with the requirements set forth in Directive/Handbook 0735 when any of the following events occur:

1. When no longer needed for contract performance.
2. Upon completion of the Contractor/subcontractor employee's employment.
3. Upon contract completion or termination.

f. Lost/stolen. Immediately upon detection, the Contractor shall report a lost or stolen
a PIV/identification card to the Government authorities as identified in Directive/Handbook 0735. Within 48 hours of reporting the lost/stolen PIV/identification card, the Contractor shall submit to the Program Manager an incident report that describes the relevant facts and circumstances regarding the loss/theft. If the loss/theft was reported by the Contractor to the local police, the Contractor shall further submit a copy of the final police report to the Program Manager within 48 hours of the report being made available by the local police department. The Government will not reimburse the Contractor for any costs that result from lost/stolen PIV/identification card(s).

g. Regular Reporting. The Contractor shall submit a status report to PIV Sponsor within 5
working days after the end of each calendar quarter and as requested by the Government in order to initiate contract closeout procedures. The report must provide the status of each contractor/subcontractor employee who is required to have a PIV/identification card during the performance of the contract. The report shall identify the Contractor and the contract number, and list the following status for each contractor/subcontractor employee who holds a PIV/identification card under this contract:

1. Contract: 1. Contractor/subcontractor employee name.
2. Name of VA facility where Contractor/subcontractor employee works, if applicable.

3. Date background check submitted for Contractor/subcontractor employee.
4. Date PIV/identification card issued to Contractor/subcontractor employee.
5. Contractor/subcontractor employee's PIV/identification card number, as applicable.
6. Date Contractor/subcontractor employee no longer has need for PIV/identification card.
7. Date Contractor notified VA that PIV/identification card is no longer required.
8. Date Contractor returned PIV/identification card was returned to VA.

h. Flow down of clause. The Contractor shall include the substance of this clause in subcontracts, third-party agreements, and BAA's, in which subcontractors, third-party servicers/employees, and business associates will perform functions where they will have physical access to a VA facility or logical access to VA data, information, VA sensitive information, or information technology or VA information system containing such data or information.

(End of Clause)

C.9 852.211-76 LIQUIDATED DAMAGES—REIMBURSEMENT FOR DATA BREACH COSTS (FEB 2023)

(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 $37.50 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 $37.50 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)

C.10 VAAR 852.222-71 COMPLIANCE WITH EXECUTIVE ORDER 13899 (APR 2025) (DEVIATION)

(a)The contractor shall comply with Executive Order 13899, Combating Anti-Semitism, pursuant to Title VI of the Civil Rights Act of 1964 (Title VI), 42 U.S.C. 2000d et seq.

(b)The contractor shall timely disclose, in writing, to the Contracting Officer, whenever, in connection with the award, performance, or closeout of this contract or any subcontract thereunder, the Contractor has credible evidence that a principal, employee, agent, or subcontractor of the Contractor has committed a violation under Executive Order 13899, Combatting Anti-Semitism pursuant to the Civil Rights Act of 1964 (Title VI), 42 U.S.C. 2000d et seq.

(c)The contractor shall include the terms and conditions of this clause in every subcontract or purchase order so that these terms will be binding on every subcontractor or vendor.

(End of clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

Attachment 1 – Amendment 0002 QA - DSS Infusion Therapy Manager Solicitation 36C10B26R0039

SECTION E - SOLICITATION PROVISIONS

E.1 FAR 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

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):

RFO/FAR: https://www.acquisition.gov/far-overhaul

VAAR: https://www.acquisition.gov/vaar

RFO Number	Title	Date
52.203-18	PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS	JAN 2017
52.204-7	SYSTEM FOR AWARD MANAGEMENT	NOV 2025
52.212-1	INSTRUCTIONS TO OFFERORS—COMMERCIAL PRODUCTS AND COMMERCIAL SERVICES	NOV 2025
852.239-75	INFORMATION AND COMMUNICATION TECHNOLOGY ACCESSIBILITY NOTICE	FEB 2023
852.273-74	AWARD WITHOUT EXCHANGES	NOV 2021

(End of Provision)

E.2 RFO 52.203-11 CERTIFICATION AND DISCLOSURE REGARDING PAYMENT TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (SEP 2024)

(a) Definitions. As used in this provision-"Lobbying contact" has the meaning provided at 2 U.S.C. 1602(8). The terms "agency," "influencing or attempting to influence," "officer or employee of an agency," "person," "reasonable compensation," and "regularly employed" are defined in the FAR clause of this solicitation entitled "Limitation on Payments to Influence Certain Federal Transactions" (52.203-12).

(b) Prohibition. The prohibition and exceptions contained in the FAR clause of this solicitation entitled "Limitation on Payments to Influence Certain Federal Transactions" (52.203-12) are hereby incorporated by reference in this provision.

(c) Certification. The offeror, by signing its offer, hereby certifies to the best of its knowledge and belief that no Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of

Congress, an officer or employee of Congress, or an employee of a Member of Congress on its behalf in connection with the awarding of this contract.

(d) Disclosure. If any registrants under the Lobbying Disclosure Act of 1995 have made a lobbying contact on behalf of the offeror with respect to this contract, the offeror shall complete and submit, with its offer, OMB Standard Form LLL, Disclosure of Lobbying Activities, to provide the name of the registrants. The offeror need not report regularly employed officers or employees of the offeror to whom payments of reasonable compensation were made.

(e) Penalties. Submission of this certification and disclosure is a prerequisite for making or entering into this contract imposed by 31 U.S.C. 1352. Any person who makes an expenditure prohibited under this provision or who fails to file or amend the disclosure required to be filed or amended by this provision, shall be subject to civil penalties as provided in 31 U.S.C. 1352. An imposition of a civil penalty does not prevent the Government from seeking any other remedy that may be applicable.

(End of provision)

E.3 52.209-12 CERTIFICATION REGARDING TAX MATTERS (OCT 2025)

(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)

E.4 RFO 52.216-1 TYPE OF CONTRACT (NOV 2025)

The Government contemplates award of a firm fixed price contract resulting from this solicitation.

(End of provision)

E.5 RFO 52.219-4 NOTICE OF PRICE EVALUATION PREFERENCE FOR HUBZONE SMALL BUSINESS CONCERNS (DEV NOV 2025)

(a) Evaluation preference.(1) Offers will be evaluated by adding a factor of 10 percent to the price of all offers, except-

(i) Offers from HUBZone small business concerns that have not waived the evaluation preference; and

(ii) Otherwise successful offers from small business concerns.

(b) Waiver of evaluation preference. A HUBZone small business concern may choose to waive the evaluation preference. If the concern waives the preference, the factor will be added to its offer for evaluation purposes.

□ Offeror chooses to waive the evaluation preference.

(c) Joint venture. A HUBZone joint venture agrees that, in the performance of the contract, at least 40 percent of the aggregate work performed by the joint venture shall be completed by the HUBZone small business parties to the joint venture. Work performed by the HUBZone small business parties to the joint venture must be more than administrative functions.

(End of provision)

E.6 RFO 52.222-90 ADDRESSING DEI DISCRIMINATION BY FEDERAL CONTRACTORS (DEV NOV 2025)

(a) Definitions. As used in this clause—

Program participation means membership or participation in, or access or admission to: training, mentoring, or leadership development programs; educational opportunities; clubs; associations; or similar opportunities that are sponsored or established by the contractor or subcontractor.

Racially discriminatory diversity, equity, and inclusion (DEI) activities means disparate treatment based on race or ethnicity in the recruitment, employment (e.g., hiring, promotions), contracting (e.g., vendor agreements), program participation, or allocation or deployment of an entity's resources.

(b) In connection with the performance of work under this contract, the Contractor agrees as follows:

(1) The Contractor will not engage in any racially discriminatory DEI activities;

(2) The Contractor will furnish all information and reports, including providing access to books, records, and accounts, as required by the Contracting Officer, for purposes of ascertaining compliance with this clause;

(3) In the event of the Contractor's or a subcontractor's noncompliance with this clause, this contract may be canceled, terminated, or suspended in whole or in part, and the Contractor or subcontractor may be declared ineligible for further Government contracts;

(4) The Contractor will report any subcontractor's known or reasonably knowable conduct that may violate this clause to the Contracting Officer and take any appropriate remedial actions directed by the Contracting Officer; and

(5) The Contractor will inform the Contracting Officer if a subcontractor sues the Contractor and the suit puts at issue, in any way, the validity of this clause.

(6) The Contractor recognizes that compliance with the requirements of this clause are material to the Government's payment decisions for purposes of 31 U.S.C. 3729(b)(4).

(c) The Contractor must include the substance of this clause, including this paragraph (c), in subcontracts at any tier, including those for commercial products and commercial services, except those where the place of delivery or performance is outside the United States.

(End of clause)

E.7 RFO 52.240-90 SECURITY PROHIBITIONS AND EXCLUSIONS REPRESENTATIONS AND CERTIFICATIONS (DEV NOV 2025)

(a) Definitions. As used in this provision-—

Backhaul, covered article, covered telecommunications equipment or services, critical technology, FASCSA order, Intelligence community, interconnection arrangements, national security system, roaming, sensitive compartmented information, sensitive compartmented information system, source, and substantial or essential component have the meanings provided in the clause 52.240-91, Security Prohibitions and Exclusions.

Business operations means engaging in commerce in any form, including by acquiring, developing, maintaining, owning, selling, possessing, leasing, or operating equipment, facilities, personnel, products, services, personal property, real property, or any other apparatus of business or commerce.

Marginalized populations of Sudan means—

(1) Adversely affected groups in regions authorized to receive assistance under section 8(c) of the Darfur Peace and Accountability Act (Pub. L. 109-344) (50 U.S.C. 1701 note); and

(2) Marginalized areas in Northern Sudan described in section 4(9) of such Act.

Restricted business operations means business operations in Sudan that include power production activities, mineral extraction activities, oil-related activities, or the production of military equipment, as those terms are defined in the Sudan Accountability and Divestment Act of 2007 (Pub. L. 110-174). Restricted business operations do not include business operations that the person (as that term is defined in Section 2 of the Sudan Accountability and Divestment Act of 2007) conducting the business can demonstrate—

(1) Are conducted under contract directly and exclusively with the regional government of southern Sudan;

(2) Are conducted under specific authorization from the Office of Foreign Assets Control in the Department of the Treasury, or are expressly exempted under Federal law from the requirement to be conducted under such authorization;

(3) Consist of providing goods or services to marginalized populations of Sudan;

(4) Consist of providing goods or services to an internationally recognized peacekeeping force or humanitarian organization;

(5) Consist of providing goods or services that are used only to promote health or education; or

(6) Have been voluntarily suspended.

Sensitive technology—

(1) Means hardware, software, telecommunications equipment, or any other technology that is to be used specifically—

(i) To restrict the free flow of unbiased information in Iran; or

(ii) To disrupt, monitor, or otherwise restrict speech of the people of Iran; and

(2) Does not include information or informational materials the export of which the President does not have the authority to regulate or prohibit pursuant to section 203(b)(3) of the International Emergency Economic Powers Act (50 U.S.C. 1702(b)(3)).

(b) Procedures.

(1) Covered telecommunications and video surveillance. The Offeror shall review the list of excluded parties in the System for Award Management (SAM) at https://www.sam.gov for entities excluded from receiving federal awards for “covered telecommunications equipment or services.”

(2) FASCSA Orders.

(i) The Offeror shall search in SAM for the phrase “FASCSA order” for any covered article, or any products or services produced or provided by a source, if there is an applicable FASCSA order described in paragraph (e) of FAR 52.240-91, Security Prohibitions and Exclusions.

(ii) The Offeror shall review the solicitation for any FASCSA orders that are not in SAM but are effective and apply to the solicitation and resultant contract (see FAR 40.204-1(c)(2)).

(iii) FASCSA orders issued after the date of solicitation do not apply unless added by an amendment to the solicitation.

(c) Covered telecommunications equipment or services representations. By submission of its offer, the Offeror represents that, after conducting a reasonable inquiry (that looks at any information in the Offeror’s possession but does not need to include an internal or third-party audit)—

(1) It will not provide covered telecommunications equipment or services to the Government in the performance of any contract, subcontract or other contractual instrument resulting from this solicitation, except as waived by the solicitation, or as disclosed in paragraph (g); and

(2) It does not use covered telecommunications equipment or services, or use any equipment, system, or service that uses covered telecommunications equipment or services, except as waived by the solicitation, or as disclosed in paragraph (g).

(d) FASCSA Representation. By submission of this offer, the offeror represents that it has conducted a reasonable inquiry, and that the offeror does not propose to provide or use in response to this solicitation any covered article, or any products or services produced or provided by a source, if the covered article or the source is prohibited by an applicable FASCSA order in effect on the date the solicitation was issued, except as waived by the solicitation, or as disclosed in paragraph (g). A reasonable inquiry will look at any information in the offeror’s possession but does not need to include an internal or third-party audit.

(e) Sudan certification. By submission of its offer, the offeror certifies, after conducting a reasonable inquiry (that looks at any information in the offeror’s possession but does not need to include an internal or third-party audit), that the offeror does not conduct any restricted business operations in Sudan.

(f) Iran Representation and Certifications.

(1) Except as provided in paragraph (f)(2) of this provision or if a waiver has been granted in accordance with FAR 40.203-3, the offeror, after conducting a reasonable inquiry (that looks at any information in the offeror's possession but does not need to include an internal or third-party audit), by submission of its offer—

(i) Represents, to the best of its knowledge and belief, that the offeror does not export any sensitive technology to the government of Iran or any entities or individuals owned or controlled by, or acting on behalf or at the direction of, the government of Iran;

(ii) Certifies that the offeror, or any person (as defined at section 15 of the Iran Sanctions Act of 1996, Pub. L. 104-172, 50 U.S.C. 1701 note) owned or controlled by the offeror, does not engage in any activities for which sanctions may be imposed under section 5 of the Act. These sanctioned activities are in the areas of development of the petroleum resources of Iran, production of refined petroleum products in Iran, sale and provision of refined petroleum products to Iran, and contributing to Iran's ability to acquire or develop certain weapons or technologies; and

(iii) Certifies that the offeror, and any person owned or controlled by the offeror, does not knowingly engage in any transaction that exceeds $15,000 with Iran's Revolutionary Guard Corps or any of its officials, agents, or affiliates, the property and interests in property of which are blocked pursuant to the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) (see OFAC's Specially Designated Nationals and Blocked Persons List at https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx)

(2) Exception for trade agreements. The representation and certification requirements of paragraph (f)(1) of this provision do not apply if—

(i) This solicitation includes a trade agreements notice or certification (e.g., 52.225-6, Trade Agreements Certificate); and

(ii) The offeror has certified that all the offered products to be supplied are designated country end products or designated country construction material.

(iii) The offeror shall email questions concerning sensitive technology to the Department of State at CISADA106@state.gov.

(g) Disclosure.

(1) If the Offeror is not able to represent compliance with the prohibitions in paragraphs (c) or (d), then the Offeror shall disclose within 72 hours to the contracting office identified in paragraph (g)(2) the following information for each product or service not compliant:

(i) Contract number and order number, if applicable;

(ii) Identification of whether this disclosure relates to paragraph (c) on covered telecommunication equipment or services, or to paragraph (d) on FASCSA orders;

(iii) A description of the products or services that the Contractor identifies or has reason to suspect is prohibited (include brand; model number, such as the original equipment manufacturer (OEM) number, manufacturer part number, or wholesaler number; and item description, as applicable);

(iv) The entity that produced the product or service (include entity name, unique entity identifier, Contractor and Government Entity (CAGE) code, facilities responsible for design, fabrication,

assembly, packaging, and test of the product, and whether the entity was the OEM or a distributor (provide manufacturer codes and distributor codes used for the product));

(v) Description of the functionality of the product or service and how that functionality impacts the risk to the product or service;

(vi) An explanation of any factors relevant to determining if the product or service should be permitted by an applicable exception, exemption, or waiver (if the offeror would like the Government to consider a waiver);

(vii) Whether alternative products or services are available that would be compliant with the prohibition;

(viii) If the product or service is related to item maintenance, include the following information on the item being maintained:

(A) Brand;

(B) Model number, OEM number, manufacturer part number, or wholesaler number; and

(C) Item description, as applicable.

(ix) Any readily available information about mitigation actions undertaken or recommended.

(2) If a disclosure is required to be submitted to a contracting office, the offeror shall submit the disclosure as follows:

(i) If a Department of Defense contracting office, the offeror shall submit the disclosure to the website at https://dibnet.dod.mil.

(ii) For all other contracting offices, the Offeror shall submit the disclosure to the Contracting Officer.

(3) If the disclosure provided does not contain any of the information required by paragraph (1), and the Offeror later discovers new information that is required by paragraph (1), then the Offeror shall submit a subsequent disclosure within 72 hours of discovering the new information.

(h) Executive agency review of disclosures. The Contracting Officer will review disclosures provided in paragraph (g) to determine if any applicable waiver may be sought. The Contracting Officer may choose not to pursue a waiver and may instead make an award to an Offeror that does not require a waiver.

(End of provision)

E.8 VAAR 852.215-72 NOTICE OF INTENT TO RE-SOLICIT (OCT 2019)

This solicitation provides offerors fewer than 30 days to submit proposals. In the event that only one offer is received in response to this solicitation, the Contracting Officer may cancel the solicitation and re-solicit for an additional period of at least 30 days in accordance with 815.370-2.

(End of provision)

E.9 VAAR 852.233-70 PROTEST CONTENT/ALTERNATIVE DISPUTE RESOLUTION (SEP 2018)

(a) Any protest filed by an interested party shall–

(1) Include the name, address, fax number, and telephone number of the protester;

(2) Identify the solicitation and/or contract number;

(3) Include an original signed by the protester or the protester's representative and at least one copy;

(4) Set forth a detailed statement of the legal and factual grounds of the protest, including a description of resulting prejudice to the protester, and provide copies of relevant documents;

(5) Specifically request a ruling of the individual upon whom the protest is served;

(6) State the form of relief requested; and

(7) Provide all information establishing the timeliness of the protest.

(b) Failure to comply with the above may result in dismissal of the protest without further consideration.

(c) Bidders/offerors and Contracting Officers are encouraged to use alternative dispute resolution (ADR) procedures to resolve protests at any stage in the protest process. If ADR is used, the Department of Veterans Affairs will not furnish any documentation in an ADR proceeding beyond what is allowed by the Federal Acquisition Regulation.

(End of provision)

E.10 VAAR 852.233-71 ALTERNATE PROTEST PROCEDURE (SEP 2018)

(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.

(End of provision)

E.11 VAAR 852.273-70 LATE OFFERS (NOV 2021)

This provision replaces paragraph (f) of FAR provision 52.212-1, Instructions to Offerors—Commercial Items. Offers or modifications of offers received after the time set forth in a request for quotations or request for proposals may be considered, at the discretion of the contracting officer, if determined to be in the best interest of the Government. Late bids submitted in response to an invitation for bid (IFB) will not be considered.

(End of provision)

E.12 INSTRUCTIONS TO OFFERORS

1. INTRODUCTION

The Offeror’s proposal shall be submitted electronically by the date and time indicated in the solicitation via email to john.sangalang@va.gov and stefanie.applegate@va.gov in the files set forth below. It is the Offeror’s responsibility to confirm the Government received proposals including all volumes and attachments. The Offeror’s proposal shall

consist of five separate volumes. The Volumes are I -Technical, II – Past Performance, III – Price, IV – Veterans Involvement and V - Solicitation, Offer and Award Documents.

The use of hyperlinks or embedded attachments in proposals is strictly prohibited. Accordingly, any hyperlinks or embedded attachments included with a proposal will neither be accessed nor viewed by the Government and thus, not evaluated as part of the Offeror's proposal submission.

WARNING: Please do not wait until the last minute to submit your proposals! Late proposals will not be accepted for evaluation. To avoid submission of late proposals, we recommend the transmission of your proposal file 24 hours prior to the required proposal due date and time. Please be advised that timeliness is determined by the date and time an Offeror's proposal is received by the Government not when an Offeror attempted transmission. Offerors are encouraged to review and ensure that sufficient bandwidth is available on their end of the transmission.

2. PROPOSAL FILES. Offeror's responses shall be submitted in accordance with the following instructions:

a. Format. The submission shall be clearly indexed and logically assembled. Each volume shall be clearly identified and shall begin at the top of a page. All pages of each volume shall be appropriately numbered and identified by the complete company name, date and solicitation number in the header and/or footer. Proposal page limitations are applicable to this procurement. The Table below indicates the maximum page count (when applicable) for each volume of the Offeror's proposal.

All files will be submitted as either a Microsoft Word 2010 (.doc) [if allowing Word documents] Microsoft Excel (.XLS) file or an Acrobat (PDF) file or compatible as indicated in the table. Page size shall be no greater than 8 1/2" x 11" with printing on one side, only. The top, bottom, left and right margins shall be a minimum of one inch (1") each. Font size shall be no smaller than 12-point. Arial or Times New Roman fonts are required. Characters shall be set at no less than normal spacing and 100% scale. Tables and illustrations may use a reduced font size not less than 8-point and may be landscape. Line spacing shall be set at no less than single space. Each paragraph shall be separated by at least one blank line. Page numbers, company logos, and headers and footers may be within the page margins ONLY and are not bound by the 12-point font requirement. Footnotes to text shall not be used. All proprietary information shall be clearly and properly marked. If the Offeror submits annexes, documentation, attachments or the like, not specifically required by this solicitation, such will count against the Offeror's page limitations unless otherwise indicated in the specific volume instructions below. Pages in violation of these instructions, either by exceeding the margin, font, printing, or spacing restrictions or by exceeding the total page limit for a particular volume, will not be evaluated. Pages not evaluated due to violation of the margin, font or spacing restrictions will not count against the page limitations. The page count will be determined by counting the pages in the order they come up in the print layout view.

b. File Packaging. All of the proposal files may be compressed (zipped) into one file entitled "proposal.zip" using WinZip version 6.2 or later version or the proposal files may be submitted individually.

c. Content Requirements. All information shall be confined to the appropriate file. The Offeror shall confine submissions to essential matters, sufficient to define the proposal and provide an adequate basis for evaluation. Offerors are responsible for including sufficient details, in a concise manner, to permit a complete and accurate evaluation of each proposal. The titles and page limits requirements for each file are shown in the Table below:

Volume Number	Factor	File Name	Page Limitations*
Volume I	Technical	Tech.pdf	10 pages
Volume II	Past Performance	Past Perf.pdf	5 pages
Volume III	Price	Price.xls	None
Volume IV	Veterans Involvement	VetsI.pdf	None
Volume V	Solicitation, Offer & Award Documents, Certifications & Representations	OfrRep.pdf	None

See also RFO 52.212-1, Instructions to Offerors – Commercial Items.

(i) VOLUME I – TECHNICAL FACTOR. Offerors shall propose a detailed approach that addresses the following:

(1) Offeror ability provide licenses, deliver software, test, implement, maintain and train on the DSS Brand Name software Infusion Therapy Manager.
(2) Offeror ability to license and maintain the DSS Brand Name software VistA Chemotherapy Manager.
(3) Implementation/Go Live Strategy containing overview of:
    a. ITM in the Oncology, Gastroenterology, Rheumatology, Neurology, Endocrinology, Infusion clinic, Inpatient, and Pharmacy settings of the facility.
    b. Education and training to ensure users know how to provide orderable item verification and treatment plan building, as well as general user and administrative functions.
    c. Education and training on how to upload or build treatment plans in ITM to meet each facility standard of care.
    d. Education and training sessions for testing and production use.
    e. On-site support during go-live implementation.
    f. System and user documentation.
    g. Contractor Project Management Plans (CPMPs)
    h. Contingency plans.

i. Training plans and educational materials.
j. Post-implementation support plan.

(4) Key Contractor Personnel listing, with relevant certifications

(ii) VOLUME II – PAST PERFORMANCE FACTOR. Offerors shall submit a list of all contracts, as well as all proposed major subcontractors (including Federal, State, and local government and private) (prime contracts, task/delivery orders, and/or major subcontracts) in performance at any point during the three (3) years immediately prior to the proposal submission date, which are relevant to the efforts required by this solicitation. Areas of relevance include previous DSS Infusion Therapy Manager installations, DSS Vista Chemotherapy Manager installations and license/maintenance contracts. Data concerning the prime contractor shall be provided first, followed by each proposed major subcontractor, in alphabetical order. This volume shall be organized into the following sections:

(1) Section 1 – Contract Descriptions. Section 1 may be provided in excel format and will not be included in the 5 page limitation as stated in section E.12(2)(c). This section shall include the following information:

(a) Contractor/Subcontractor place of performance, CAGE Code and DUNS Number. If the work was performed as a subcontractor, also provide the name of the prime contractor and Point of Contact (POC) within the prime contractor organization (name, and current address, e-mail address, and telephone and fax numbers).

(b) Contracting activity, and current address, Procuring Contracting Officer's name, e-mail address, telephone and fax numbers.

(c) Technical representative/Contracting Officer’s Representative (COR), and current e-mail address, telephone and fax numbers.

(d) Contract administration activity and the Administrative Contracting Officer's name, and current e-mail address, telephone and fax numbers.

(e) Contract Number and, in the case of Indefinite Delivery type contracts, GSA contracts, and Blanket Purchase Agreements, include Delivery Order Numbers also.

(f) Contract Type (specific type such as Fixed Price (FP), Cost Reimbursement (CR), Time & Materials (T&M), etc.) In the case of Indefinite Delivery contracts, indicate specific type (Requirements, Definite Quantity, and Indefinite Quantity) and secondary contract type (FP, CR, T&M, etc.)).

(g) Awarded price/cost.

(h) Final or projected final price/cost.

(i) Original delivery schedule, including dates of start and completion of work.

(j) Final or projected final, delivery schedule, including dates of start and completion of work.

(2) Section 2 - Performance. Offerors shall provide a specific narrative explanation of each contract listed in Section 1 describing the objectives achieved and detailing how the effort is relevant to the requirements of this solicitation. For any contract(s)/task order(s) that did not/do not meet original schedule or technical performance requirements, provide a brief explanation of the reason(s) for the shortcoming(s) and any corrective action(s) taken to avoid recurrence. The Offerors shall list each time the delivery schedule was revised and provide an explanation of why the revision was necessary. The Offerors shall indicate if any of the contracts listed were terminated and the type and reasons for the termination.

(3) Section 3 – Subcontracts. Offerors shall provide an outline of how the effort required by the solicitation will be assigned for performance within the Offeror's corporate entity and among the proposed subcontractors. The information provided for the prime Offeror and each proposed major subcontractor must include the entire company name, company address, CAGE Code, DUNS Number and type of work to be performed by citing the applicable Government PWS paragraph number.

(4) Section 4 – New Corporate Entities. New corporate entities may submit data on prior contracts involving its officers and employees. However, in addition to the other requirements in this section, the Offeror shall discuss in detail the role performed by such persons in the prior contracts cited. Information should be included in the files described in the sections above.

(iii) VOLUME III– PRICE FACTOR

This is a FFP single award ID/IQ contract.

a) The Offeror shall complete and submit section B.2 Price Schedule of the solicitation and submit with their proposal. The Government will review the calculations and adjust the evaluated price if there are errors.

b) Price Rounding Issue - The Government requires Offerors to propose unit prices and total prices that are two (2) decimal places and requires the unit prices and total prices to be displayed as two (2) decimal places. Ensure that the two (2) digit unit price multiplied by the item quantity equals the two (2) digit total item price (there should be no rounding). No Spreadsheet is required.

All Offerors should propose using an estimated award date of September 30, 2026.

(iv) VOLUME IV – VETERANS INVOLVEMENT FACTOR.

(1) For SDVOSBS/VOSBs: In order to receive credit under this Factor, an Offeror shall submit a statement of compliance that it qualifies as a SDVOSB or VOSB in accordance with VAAR 852.215-70, Service-Disabled Veteran-Owned and Veteran-Owned Small Business Evaluation Factors (DEVIATION). Offerors are cautioned that they must be registered and verified in the Small Business Administration VetCert database (https://veterans.certify.sba.gov) and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and at time of award. The Government may contact the Offeror to obtain a copy of the Small Business Administration Letter confirming the business certification status.

(2) For Non-SDVOSBs/VOSBs: To receive some consideration under this Factor, an Offeror must state in its proposal the names of SDVOSB(s) and/or VOSB(s) with whom it intends to subcontract and provide a brief description and the approximate dollar values of the proposed subcontracts. Additionally, proposed SDVOSB/VOSB subcontractors must be registered and verified in the Small Business Administration VetCert database (https://veterans.certify.sba.gov) in order to receive some consideration under the Veteran's Involvement Factor and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of proposal submission and time of award. The Government may contact the Offeror to obtain a copy of the Small Business Administration Letter confirming the business certification status.

(v) VOLUME V - SOLICITATION, OFFER AND AWARD DOCUMENTS AND CERTIFICATIONS/REPRESENTATIONS.

Certifications and Representations – An authorized official of the firm shall sign the Standard Form (SF) 1449 and all certifications requiring original signature. An Acrobat PDF file shall be created to capture the signatures for submission. This Volume shall contain the following:

a. Solicitation Section A – SF1449 and Acknowledgement of Amendments, if any.

b. Artificial Intelligence Efforts:

Response Instructions: Offerors shall, if Artificial Intelligence (AI) is part of the Contractor system/solution, provide the below self-certification with their quote/proposal affirming that the identified/proposed AI System/LLM complies with the two Unbiased AI Principles, Truth-seeking and Ideological Neutrality, as required by the Office of Management and Budget (OMB) Memorandum M-26-04, "Increasing Public Trust in Artificial Intelligence Through Unbiased AI Principles", or indicate otherwise that a self-certification is Not Applicable. Additionally, Offerors shall self-certify that the content requested within the AI System/LLM Development and Operation Documentation, as identified in OMB Memorandum M-26-04 as Transparency Documentation, will be provided for its proposed AI System/LLM during the period of performance, meet the required transparency threshold and align with the two Unbiased AI Principles. Failure to include the requisite Offeror's self-certification may render the Offeror's proposal/quotation unacceptable, and therefore ineligible for award. The Government will rely on the Offeror's self-certification that its proposed AI System/LLM adheres to the Unbiased AI Principles and related requirements. VA reserves the right to request additional information if it determines that doing so is in the Government's best interest.

Certification:

☐ Not Applicable

☐ I hereby certify that the proposed AI System/LLM complies with the required Unbiased AI Principles as identified in OMB Memorandum M-26-04 and can also meet the required AI System/LLM Development and Operation Documentation requirements specified therein. I further certify that I am authorized to execute this certification on behalf of *<insert name of Offeror>*.

Printed Name of Signee: _____

Printed Title of Signee: _____

Signature: _____

Name (and version) of its proposed AI System/LLM: _____

_____

Date: _____

Company Name and Address: _____

_____

---

c. Any proposed terms and conditions and/or assumptions upon which the offer/quotation is predicated. The Government will not be held to any terms and conditions and/or assumptions found in any other Volume and is not responsible for reviewing other Volumes for any terms and conditions and/or assumptions.

E.13 BASIS OF AWARD

A. BASIS FOR AWARD
Any award will be made based on the best overall (i.e., best value) proposal that is determined to be the most beneficial to the Government, with appropriate consideration given to the four following evaluation factors: Technical, Past Performance, Price, and Veterans Involvement. The Technical Factor is significantly more important than the Past Performance Factor, which is more important than the Price Factor, which is more important than the Veterans Involvement Factor. To receive consideration for award, a rating of no less than "Acceptable" must be achieved for the Technical Factor. The non-Price Factors combined are significantly more important than the Price Factor. Offerors are cautioned that any resulting award may not necessarily be made to the lowest Price offered or the most highly rated technical proposal. The Government intends to award one contract to one vendor.

B. FACTORS TO BE EVALUATED

1. TECHNICAL
2. PAST PERFORMANCE
3. PRICE
4. VETERANS INVOLVEMENT

C. EVALUATION APPROACH - All proposals shall be subject to evaluation by a team of Government personnel. The Government reserves the right to award without discussions based upon the initial evaluation of proposals. The proposal will be evaluated strictly in accordance with its written content. Proposals which merely restate the requirement or state that the requirement will be met, without providing supporting rationale, are not sufficient. Offerors who fail to meet the minimum requirements of the solicitation will be rated Unacceptable and thus, ineligible for award.

1. TECHNICAL EVALUATION APPROACH. The evaluation process will consider the following:

a. Understanding of the Problem - The proposal will be evaluated to determine the extent to which it demonstrates a clear understanding of all features involved in solving the problems and meeting and/or exceeding the requirements presented in the solicitation and the extent to which uncertainties are identified and resolutions proposed.

b. Feasibility of Approach - The proposal will be evaluated to determine the extent to which the proposed approach is workable and the end results achievable. The proposal will be evaluated to determine the level of confidence provided the Government with respect to the Offeror's methods and approach in successfully meeting and/or exceeding the requirements in a timely manner.

2. PAST PERFORMANCE EVALUATION APPROACH.

The Past Performance evaluation will assess the relative risks associated with an Offeror's likelihood of success in fulfilling the solicitation's requirements as indicated by that Offeror's record of past performance. In this context, “Offeror” refers to the

proposed prime contractor and all proposed major subcontractor(s). A major subcontractor is defined as one who will be providing critical installation and training services and/or whose subcontract is for more than 51% of the total proposed price. In either case, the prime contractor and proposed major subcontractor(s) will be assessed individually and the results will then be assessed in their totality to derive the Offeror's Past Performance rating.

The Government will conduct a performance risk assessment based on the quality, relevancy, and recency of the Offeror's past performance, as well as that of its major subcontractors, as it relates to the probability of successful accomplishment of the required effort. Offerors are cautioned that the Government will review available past performance data available in the Contractor Performance Assessment Reporting System (CPARS). The Government reserves the right to obtain past performance information from any available source and may contact customers other than those identified by the Offeror when evaluating past performance. Since the Government may not necessarily interview all of the sources provided by the Offerors, it is incumbent upon the Offerors to explain the relevance of the data provided. Offerors are reminded that the burden of proving low performance risk rests with the Offerors.

The Government will review aspects of cost, schedule, and performance. Areas to be evaluated may include, but are not limited to, quality of product or service, timeliness of performance or adherence to delivery schedules, and/or effectiveness in program management (to include use and control of subcontractors).

In the case of an Offeror without a record of relevant past performance or for whom information on past performance is not available, the Offeror may not be evaluated favorably or unfavorably on Past Performance.

3. PRICE EVALUATION APPROACH.

*NOTE: For non-small business set-asides, the RFO requires the use of a HUBZone Price Evaluation Adjustment pursuant to RFO 52.219-4.

For Offerors from HUBZone business concerns that have not waived the evaluation preference, a price evaluation preference will be applied in accordance with RFO 52.219-4.

Fixed Price: The Government will evaluate the price by adding the total of all line item prices, including all options. The Total Evaluated Price will be that sum.

Unbalanced Pricing - The Government may evaluate whether the Offeror has submitted unbalanced pricing. An unbalanced price is one where the price of one or more contract line items is significantly overstated or understated and which will result in the Government paying an unreasonably high price for contract performance or otherwise present an unacceptable level of risk to the Government. If the Contracting Officer determines that the risk is unacceptable, then the bid or offer can be rejected.

4. VETERANS INVOLVEMENT EVALUATION APPROACH.

In accordance with Veterans Affairs Acquisition Regulation (VAAR) 852.215-70 (DEVIATION), Service-Disabled Veteran-Owned and Veteran-Owned Small Business (VOSB) Evaluation Factors, the Government will assign evaluation credit for an Offeror

(prime contractor) which is a Service-Disabled Veteran-Owned Small Business (SDVOSB) or a VOSB. To receive credit, an offeror must be registered and verified in Small Business Administration VetCert database (https://veterans.certify.sba.gov) database at time of proposal submission and at time of award, must meet federal small business size standards for the North American Industry Classification System (NAICS) code assigned to this solicitation.

Non-SDVOSB/VOSB Offerors proposing to use SDVOSBs or VOSBs as subcontractors will receive some consideration under this evaluation Factor. Offerors must state in their proposals the names of the SDVOSBs and VOSBs with whom they intend to subcontract and provide a brief description of the proposed subcontracts and the approximate dollar values of the proposed subcontracts. In proposed subcontractors must be registered and verified in the Small Business Administration VetCert database (https://veterans.certify.sba.gov) and must meet federal small business size standards for the NAICS code assigned to this solicitation at time of both proposal submission and at time of award. The Government may contact the Offeror to obtain a copy of the Small Business Administration Letter confirming the business certification status.

SECTION H - SPECIAL CONTRACT REQUIREMENTS

H.1 ARTIFICIAL INTELLIGNENCE IN VA CONTRACTS

For purposes of this clause, AI is defined as set forth by VA and Section 238(g) of the National Defense Authorization Act for Fiscal Year 2019 to include:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning (ML), that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

The Contractor shall provide a list of all AI it will be proposing, creating, delivering, and/or using as part of contract performance, for VA approval. The list of AI shall be provided directly to the VA PM, COR, and CO at least annually but also at the following times: upon proposal submission, contract award, the COR's request, and upon the Contractor's proposed use of new AI tools not contemplated at the time of last reporting. AI shall not be used in performance of the contract without the written approval and authorization of the CO. The Contractor shall also report all AI intended for use in contract performance for VA's inclusion in the VA AI Use Case Inventory. The Contractor shall actively engage in AI discovery, assessment, and compliance activities undertaken by VA.

Once the Contractor has obtained CO authorization to use specific AI in contract performance, the Contractor shall provide the COR a signed Statement of Attestation prior to AI implementation. All AI for delivery and/or use in performance of the contract shall adhere to the *VA Trustworthy AI Framework*, available at https://department.va.gov/ai/trustworthy/. The Statement of Attestation shall include, but is not limited to, a description of all controls, processes, technologies, and mechanisms utilized to satisfy VA's six (6) AI Principles: Purposeful, Effective and Safe, Secure and Private, Fair and Equitable, Transparent and Explainable, and Accountable and Monitored. The Statement of Attestation shall also certify that the Contractor owns or possesses all legally required rights, copyright, and licenses to use the specified AI. The Statement of Attestation shall clearly state that the use of the AI by VA personnel in performance of the contract:

1. Does not and will not infringe upon any intellectual property rights of any kind.
2. Does not violate any intellectual property rights of any kind.
3. Does not violate any other third-party rights of any kind.

The Statement of Attestation shall also affirm that there have not been any persisting or existing material errors, defects, failures, or interruptions in AI performance of its

intended purpose. Additionally, the Statement of Attestation shall include the Contractor's endorsement that the AI has materially performed in accordance with its specifications and intended purpose. Lastly, the Statement of Attestation shall be updated and resubmitted, at a minimum, annually, prior to the exercise of any contract option periods. The Statement of Attestation shall be deemed separate from, and in addition to, the Contractor's reporting requirements relative to the use of AI. The Statement of Attestation is a material term of the contract; accordingly, failure to provide the Statement of Attestation, to include all requirements, may be deemed a breach of contract and thus, cause for termination.

Data Ownership and Use. VA data ("Data") shall include data collected, used, processed, stored, or generated as the result of the use of AI. VA data is and shall remain the sole and exclusive property of VA. Contractor is provided a limited, non-exclusive license to access and use Data solely for performing its obligations under the Contract. The Contractor shall: (a) keep and maintain VA data in strict confidence and as further described in this Contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) not use, sell, rent, transfer, distribute, or otherwise disclose or make available VA Data for Contractor's own purposes or for the benefit of anyone other than VA without the CO's prior written consent; and (c) not store, use, and transmit VA Data outside of the United States. This applies to both identified and de-identified data.

The Contractor (or Subcontractor at any tier, including affiliates, third-party affiliates, and any other non-VA entities) shall not sell, monetize, release, share, reuse, transfer, or misuse any VA data, to include any models, training data, testing data, patterns, documentation, implementation artifacts, runtime artifacts, or any other digital artifacts, partially or as a whole, derived from AI or machine learning (ML) without the express written consent and approval from the CO.

The Contractor is prohibited from using non-public VA data, including Veteran data, and outputted results to train publicly or commercially available AI algorithms, fine-tune, or otherwise develop AI or ML models for reuse, transfer, or commercial purposes, without the express written authorization from the CO specifying VA data that may be used along with the acceptable scope of such usage. Contractor agrees that any AI models, weights, or derivative artifacts trained, or fine-tuned, on VA non-public data, if authorized by VA, may not be commercialized or used for the benefit of any third party without prior written approval by the CO and must be conducted within a VA authorized environment that has obtained an Authority to Operate

The Contractor shall indemnify VA and its officers, employees, and agents against liability, including costs, for actual or alleged direct or contributory infringement of, or inducement to infringe, any United States or foreign patent, trademark, or copyright, arising out of VA use of any AI products and/or services under the contract.

The Contractor shall maintain commercially reasonable insurance coverage for claims or losses pertaining to the AI products or services being used in performance of the contract.

The Contractor shall maintain commercially reasonable and industry standard conforming security safeguards and controls, including proper access controls for the

AI. The Contractor agrees the VA Contracting Officer has the unilateral right to require deactivation of any AI for any reason and without notice.

Any development and/or creation of AI, including any AI derivatives, during performance of this contract, is subject to applicable Intellectual Property and data rights clauses under the Federal Acquisition Regulation (FAR) including, FAR 52.227-14. The VA retains the unlimited right to reuse, share, and/or redeploy AI code and AI models procured under this contract. License rights in any Commercial Computer Software shall be governed by this contract.

This clause applies to both existing and new uses of AI, both stand-alone AI and AI embedded within other systems or applications, AI developed both by VA or by third parties on behalf of agencies for the fulfilment of specific VA missions, including relevant data inputs used to train AI and outputs used in support of decision making, and VA procurement of AI applications.

This clause does not apply to AI embedded within common commercial products, such as word processors or map navigation systems. The Contractor shall inform the VA Contracting Officer in writing if it believes the AI it intends to use during contract performance is not covered by this clause. The burden to demonstrate the AI is a common commercial product shall rest solely with the Contractor.

Non-compliance with the terms above, or loss of sensitive VA medical records information resulting from AI use (whether accidental or intentional), may result in Contractor liability to VA for any and all rights and remedies provided by law, including but not limited to contract termination, liquidated damages, and referral to VA’s Suspension and Debarment Committee.

The Contractor shall include the substance of this clause in all subcontracts, including Subcontractors at any tier, affiliates, third-party affiliates, and any other non-VA entities.