36C10B18R2930

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

1. REQUISITION NO.
702-18-4-7071-0244

PAGE 1 OF 89

2. CONTRACT NO.
36C10B18C2930

3. AWARD/EFFECTIVE DATE
9/6/18

4. ORDER NO.

5. SOLICITATION NUMBER
36C10B18R2930

6. SOLICITATION ISSUE DATE

7. FOR SOLICITATION INFORMATION CALL:
a. NAME
Joe Jones/joseph.jones6@va.gov
b. TELEPHONE NO. (No Collect Calls)
792-795-1070

8. OFFER DUE DATE/LOCAL TIME

9. ISSUED BY CODE

Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

10. THIS ACQUISITION IS □ UNRESTRICTED OR □ SET ASIDE: % FOR:
□ SMALL BUSINESS
□ HUBZONE SMALL BUSINESS
□ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
□ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
□ EDWOSB
□ 8(A)
NAICS: 541511
SIZE STANDARD: $27.5 Million

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED
☒ SEE SCHEDULE

12. DISCOUNT TERMS

□ 13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING
N/A

14. METHOD OF SOLICITATION
□ RFQ □ IFB ☒ RFP

15. DELIVER TO CODE

See Section B

16. ADMINISTERED BY CODE

Department of Veterans Affairs
Technology Acquisition Center

23 Christopher Way
Eatontown NJ 07724

17a. CONTRACTOR/OFFEROR CODE 64EX2 FACILITY CODE

KEVADIYA INC.

2001 CENTER POINT PKWY SUITE 103

PONTIAC MI 48341

TELEPHONE NO

DUNS 963353[illegible] DUNS+4:

18a. PAYMENT WILL BE MADE BY CODE

Department of Veterans Affairs
Technology Acquisition Center
Financial Services Center
PO Box 149971
Austin TX 78714-8971

PHONE: FAX:

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

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

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	See CONTINUATION Page				
	VetRide Hosted Transportation Solution Bridge POC: Debra G. Clayton/Contracting Officer/732-795-1015 debra.clayton2@va.gov Joe Jones/Contract Specialist/732-795-1070 joseph.jones6@va.gov See section B.3 for list of specifications PO#702-C80075 Period of Performance: September 9, 2018 - March 8, 2019 with two 6-month option periods				

(Use Reverse and/or Attach Additional Sheets as Necessary)

25. ACCOUNTING AND APPROPRIATION DATA See CONTINUATION Page
702-3680160-7071-829800-2560 SPG0EP1A1

26. TOTAL AWARD AMOUNT (For Govt. Use Only)
$2,157,150.00

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

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

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

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

30a. SIGNATURE OF OFFEROR/CONTRACTOR
Nilesh Patel
Digitally signed by Nilesh Patel
Date: 2018.09.06 12:26:41 -04'00'

31a. UNITED STATES OF AMERICA (SIGNATURE OF CONTRACTING OFFICER)

30b. NAME AND TITLE OF SIGNER (TYPE OR PRINT)
Nilesh Patel, VP Eng.

30c. DATE SIGNED
09/06/2018

31b. NAME OF CONTRACTING OFFICER (TYPE OR PRINT)
Debra G. Clayton
Contracting Officer

31c. DATE SIGNED
9/6/18

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

Table of Contents

SECTION B - CONTINUATION OF SF 1449 BLOCKS

B.1 CONTRACT ADMINISTRATION DATA

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

a. CONTRACTOR: Kevadiya, Inc.
Nilesh Patel, 248-987-2843, nilesh@kevadiya.com
2001 Centerpoint Pkwy, STE 111
Pontiac, MI 48341

b. GOVERNMENT: Contracting Officer 36C10B
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] Invoices shall be submitted monthly.

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.

Department of Veterans Affairs
Technology Acquisition Center
Financial Services Center
PO Box 149971
Austin TX 78714-8971

B.2 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 U.S.C. § 5725), and FAR clauses 52.212-4, 52.227-14, 52.227-19 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. Claims of patent or copyright infringement brought against the Government as a party shall be defended by the U.S. Department of Justice (DOJ). 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 contract/order modification (Standard Form 30) and shall only be affected by a warranted Contracting Officer. Nothing in this Contract/Order or any commercial license agreement shall be construed as a waiver of sovereign immunity.

SOFTWARE LICENSE, MAINTENANCE 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 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 or 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/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.ppirs.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 or order at no cost.

B.3 SCHEDULE OF SUPPLIES/SERVICES

Base Year Period of Performance: September 9, 2018 through March 8, 2019					
Line Item	**Description**	**QTY**	**Unit**	**Unit Price**	**Total Price**
0001	Project Management shall be provided in accordance with (IAW) Performance Work Statement (PWS) paragraph 5.1. This Firm-Fixed Price (FFP) Contract Line Item Number (CLIN) includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.1.	6	MO	NSP	NSP
0001AA	Contractor Project Management Plan IAW PWS paragraph 5.1.1 This Firm-Fixed Price (FFP) Contract Line Item Number (CLIN) includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.1.	1	EA	NSP	NSP

0001AB	Kick off Meeting Agenda IAW PWS paragraph 5.1.2 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.2.	1	EA	NSP	NSP
0001AC	Kick off Meeting Minutes IAW PWS paragraph 5.1.2 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.2.	1	EA	NSP	NSP
0001AD	Weekly Progress Reports IAW PWS paragraph 5.1.3 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.3.	26	EA	NSP	NSP

0002	VetRide Scheduling Software License Subscription IAW PWS paragraph 5.2 and all subparagraphs. This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2, inclusive of all subparagraphs.	110	EA (VA site)	$15,000.00	$1,650,000.00
0003	Administrative Portal IAW PWS paragraph 5.3 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.3, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	6	MO	$10,000.00	$60,000.00

0004	Third party portal IAW PWS paragraph 5.4 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.4, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	6	MO	$5,000.00	$30,000.00
0005	Veteran Self-Service Portal IAW PWS paragraph 5.5 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.5, inclusive of all subparagraphs. The contract provides for submission of	6	MO	$5,000.00	$30,000.00

	monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
0006	Mobile Data Computer IAW PWS paragraph 5.6 and all subparagraphs This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.6, inclusive of all subparagraphs.	70	EA	$750.00	$52,500.00
0007	System Hosting IAW PWS paragraph 5.7 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.7, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval	6	MO	NSP	NSP

	of invoices for payment shall be subject to contractor's successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
0008	Data Collection and Reporting IAW PWS paragraph 5.8 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.8, inclusive of all subparagraphs.	6	MO	NSP	NSP
0009	Help Desk Services IAW PWS paragraph 5.9 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.9, inclusive of all subparagraphs.	6	MO	NSP	NSP
0010	Onsite Installation Services IAW PWS paragraph 5.2.3 This FFP CLIN includes all labor, materials, travel, and	10	EA (VA site)	$1,200.00	$12,000.00

	deliverables required for the successful completion of the services detailed in PWS paragraph 5.2.3, inclusive of all subparagraphs.				
0011	Training IAW PWS paragraph 5.10 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.10, inclusive of all subparagraphs.	10	EA	NSP	NSP
0012	Communication Services IAW PWS paragraph 5.11			See below	See below
0012AA	Satellite and Cellular Communication Services This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.11, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of	525 EA (service plan)	6 MO	$59.00	$185,850.00

	task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
0012AB	Cellular Communication Services This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.11, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor's successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	950 EA (service plan)	6 MO	$24.00	$136,800.00
BASE PERIOD TOTAL					**$2,157,150.00**

OPTION PERIOD ONE Period of Performance: If exercised, Option Period One shall be March 9, 2019 through September 8, 2019 This option may be exercised in accordance with FAR 52.217-9					
Line Item	**Description**	**QTY**	**Unit**	**Unit Price**	**Total Price**
1001	Project Management shall be provided in accordance with (IAW) Performance Work Statement (PWS) paragraph 5.1.	1	LO	NSP	NSP
1001AA	Contractor Project Management Plan updates IAW PWS paragraph 5.1.1 This Firm-Fixed Price (FFP) Contract Line Item Number (CLIN) includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.1.	1	LO	NSP	NSP
1001AD	Weekly Progress Reports IAW PWS paragraph 5.1.3 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.3. The contract provides for submission of monthly invoices. Government approval	26	EA	NSP	NSP

	of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
1002	VetRide Scheduling Software License Subscription IAW PWS paragraph 5.2 and all subparagraphs. This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2, inclusive of all subparagraphs.	110	EA (VA site)	$15,000.00	$1,650,000.00
1003	Administrative Portal IAW PWS paragraph 5.3 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.3, inclusive of all subparagraphs. The contract provides for submission of	6	MO	$10,000.00	$60,000.00

	monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
1004	Third party portal IAW PWS paragraph 5.4 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.4, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	6	MO	$5,000.00	$30,000.00

1005	Veteran Self-Service Portal IAW PWS paragraph 5.5 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.5, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor's successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	6	MO	$5,000.00	$30,000.00
1006	Mobile Data Computer IAW PWS paragraph 5.6 and all subparagraphs This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.6, inclusive of all subparagraphs.	70	EA	$750.00	$52,500.00

1007	System Hosting IAW PWS paragraph 5.7 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.7, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor's successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	6	MO	NSP	NSP
1008	Data Collection and Reporting IAW PWS paragraph 5.8 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.8, inclusive of all subparagraphs.	6	MO	NSP	NSP

1009	Help Desk Services IAW PWS paragraph 5.9 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.9, inclusive of all subparagraphs.	6	MO	NSP	NSP
1010	Onsite Installation Services IAW PWS paragraph 5.2.3 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2.3, inclusive of all subparagraphs.	10	EA (VA site)	$1,200.00	$12,000.00
1011	Training IAW PWS paragraph 5.10 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.10, inclusive of all subparagraphs.	10	EA	NSP	NSP
1012	Communication Services IAW PWS paragraph 5.11			See below	See below

1012AA	Satellite and Cellular Communication Services This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.11, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	550 EA (service plan)	6 MO	$59.00	$194,700.00
1012AB	Cellular Communication Services This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.11, inclusive of all subparagraphs.	1020 EA (service plan)	6 MO	$24.00	$146,880.00

	The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor's successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
OPTION PERIOD ONE TOTAL					**$2,176,080.00**

OPTION PERIOD TWO

Period of performance: If exercised, Option Period Two shall be September 9, 2019 through March 8, 2020

This option may be exercised in accordance with FAR 52.217-9

Line Item	Description	QTY	Unit	Unit Price	Total Price
2001	Project Management shall be provided in accordance with (IAW) Performance Work Statement (PWS) paragraph 5.1.	1	LO	NSP	NSP
2001AA	Contractor Project Management Plan updates IAW PWS paragraph 5.1.1 This Firm-Fixed Price (FFP) Contract Line Item Number (CLIN) includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.1.	1	LO	NSP	NSP
2001AD	Weekly Progress Reports IAW PWS paragraph 5.1.3 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.1.3. The contract provides for submission of monthly invoices. Government approval	26	EA	NSP	NSP

	of invoices for payment shall be subject to contractor's successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
2002	VetRide Scheduling Software License Subscription IAW PWS paragraph 5.2 and all subparagraphs. This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2, inclusive of all subparagraphs.	120	EA (VA site)	$15,000.00	$1,800,000.00
2003	Administrative Portal IAW PWS paragraph 5.3 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.3, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject	6	MO	$10,000.00	$60,000.00

	to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
2004	Third party portal IAW PWS paragraph 5.4 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.4, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	6	MO	$5,000.00	$30,000.00
2005	Veteran Self-Service Portal IAW PWS paragraph 5.5 This FFP CLIN includes all labor, materials,	6	MO	$5,000.00	$30,000.00

	travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.5, inclusive of all subparagraphs.				
2006	Mobile Data Computer IAW PWS paragraph 5.6 and all subparagraphs This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.6, inclusive of all subparagraphs.	70	EA	$750.00	$52,500.00
2007	System Hosting IAW PWS paragraph 5.7 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.7, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the	6	MO	NSP	NSP

	month for which the invoice is submitted.				
2008	Data Collection and Reporting IAW PWS paragraph 5.8 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.8, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor’s successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	6	MO	NSP	NSP
2009	Help Desk Services IAW PWS paragraph 5.9 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.9,	6	MO	NSP	NSP

	inclusive of all subparagraphs.				
2010	Onsite Installation Services IAW PWS paragraph 5.2.3 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.2.3, inclusive of all subparagraphs.	10	EA (VA site)	$1,200.00	$12,000.00
2011	Training IAW PWS paragraph 5.10 This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.10, inclusive of all subparagraphs.	10	EA	NSP	NSP
2012	Communication Services IAW PWS paragraph 5.11			See below	See below
2012AA	Satellite and Cellular Communication Services This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.11, inclusive of all subparagraphs. The contract provides for submission of	550 EA (service plan)	6 MO	$59.00	$194,700.00

	monthly invoices. Government approval of invoices for payment shall be subject to contractor's successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.				
2012AB	Cellular Communication Services This FFP CLIN includes all labor, materials, travel, and deliverables required for the successful completion of the services detailed in PWS paragraph 5.11, inclusive of all subparagraphs. The contract provides for submission of monthly invoices. Government approval of invoices for payment shall be subject to contractor's successful completion of task requirements and associated deliverables required by the PWS for the month for which the invoice is submitted.	1090 EA (service plan)	6 MO	$24.00	$156,960.00
OPTION PERIOD TWO TOTAL					**$2,336,160.00**

GRAND TOTAL (BASE PLUS OPTION PERIOD ONE + OPTION PERIOD TWO)	**$6,669,390.00**

B.4 PERFORMANCE WORK STATEMENT

1.0 BACKGROUND

Beginning in the spring of 2015, Department of Veterans Affairs (VA), Veterans Health Administration, Member Services (MS) Veterans Transportation Program (VTP) began deploying the VetRide Transportation Solution which VTP has dubbed (and referred to in this PWS) as the "VetRide" scheduling software and routing systems to the VA medical centers (VAMCs). VA requires subscription service of the existing integrated transportation approach with vehicle tracking devices, passenger tracking, dynamic routing, detailed scheduling and reporting. Transportation Services in the VA are widely dispersed and operate independently of each other. The Veterans Transportation Service (VTS) Program has provided a potential "first' step in creation of transportation services through which an optimal and cost-effective ride is brokered and managed. VTS operates under the VTP.

VAMCs currently coordinate local efforts to provide transportation services to Veterans, including specialized services to meet the specific needs of Veterans in each VAMCs catchment area. VA also provides reimbursement for medically related travel to eligible Veterans. The VTS Program is currently underway at 104 VAMC's and includes over 1,240 vehicles, 1,573 users, and transports over 500,000 Veterans annually. Even with these efforts, the VA recognizes that access to VA's benefits and services sometimes remains difficult. In some cases, VAMCs even use mobile clinics to provide services. Currently the VTP program supports 104 VMAC's with a goal of reaching 172 VAMC's and increasing access to care for Veterans nationally.

The VA seeks to improve access to health care through a subscription service to VetRide which will be located at www.vetride.va.gov. VetRide has provided a systematic approach to providing Veterans with rides to and from VA health care facilities. Transportation services are improved by providing VA health care facilities staff to support ride coordination, ride scheduling/routing and driving. Additionally, VA acquires vehicles with adequate capacity to handle shuttle and door-to-door routes. The acquired vehicles also accommodate service dogs/animals, wheel chairs, or walkers for Veterans with difficulty walking.

2.0 APPLICABLE DOCUMENTS

In the performance of the tasks associated with this Performance Work Statement, the Contractor shall comply with the following:

1. 44 U.S.C. § 3541-3549, "Federal Information Security Management Act (FISMA) of 2002"
2. "Federal Information Security Modernization Act of 2014"
3. Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements For Cryptographic Modules"
4. FIPS Pub 199. Standards for Security Categorization of Federal Information and Information Systems, February 2004
5. FIPS Pub 200, Minimum Security Requirements for Federal Information and Information Systems, March 2016
6. FIPS Pub 201-2, "Personal Identity Verification of Federal Employees and Contractors," August 2013
7. 10 U.S.C. § 2224, "Defense Information Assurance Program"
8. Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Development (CMMI-DEV), Version 1.3 November 2010; and Carnegie Mellon Software Engineering Institute, Capability Maturity Model® Integration for Acquisition (CMMI-ACQ), Version 1.3 November 2010
9. 5 U.S.C. § 552a, as amended, "The Privacy Act of 1974"

10. Public Law 109-461, Veterans Benefits, Health Care, and Information Technology Act of 2006, Title IX, Information Security Matters
11. 42 U.S.C. § 2000d "Title VI of the Civil Rights Act of 1964"
12. VA Directive 0710, "Personnel Security and Suitability Program," June 4, 2010, http://www.va.gov/vapubs/
13. VA Handbook 0710, Personnel Security and Suitability Security Program, May 2, 2016, http://www.va.gov/vapubs
14. VA Directive and Handbook 6102, "Internet/Intranet Services," July 15, 2008
15. 36 C.F.R. Part 1194 "Electronic and Information Technology Accessibility Standards," July 1, 2003
16. Office of Management and Budget (OMB) Circular A-130, "Managing Federal Information as a Strategic Resource," July 28, 2016
17. 32 C.F.R. Part 199, "Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)"
18. An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, October 2008
19. Sections 504 and 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220), August 7, 1998
20. Homeland Security Presidential Directive (12) (HSPD-12), August 27, 2004
21. VA Directive 6500, "Managing Information Security Risk: VA Information Security Program," September 20, 2012
22. VA Handbook 6500, "Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program," March 10, 2015
23. VA Handbook 6500.1, "Electronic Media Sanitization," November 03, 2008
24. VA Handbook 6500.2, "Management of Breaches Involving Sensitive Personal Information (SPI)", July 28, 2016
25. VA Handbook 6500.3, "Assessment, Authorization, And Continuous Monitoring Of VA Information Systems," February 3, 2014
26. VA Handbook 6500.5, "Incorporating Security and Privacy in System Development Lifecycle", March 22, 2010
27. VA Handbook 6500.6, "Contract Security," March 12, 2010
28. VA Handbook 6500.8, "Information System Contingency Planning", April 6, 2011
29. OI&T Process Asset Library (PAL), https://www.va.gov/process/ . Reference Process Maps at https://www.va.gov/process/maps.asp and Artifact templates at https://www.va.gov/process/artifacts.asp
30. One-VA Technical Reference Model (TRM) (reference at https://www.va.gov/trm/TRMHomePage.aspx)
31. VA Directive 6508, "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," October 15, 2014
32. VA Handbook 6508.1, "Procedures for Privacy Threshold Analysis and Privacy Impact Assessment," July 30, 2015
33. VA Handbook 6510, "VA Identity and Access Management", January 15, 2016
34. VA Directive 6300, Records and Information Management, February 26, 2009
35. VA Handbook, 6300.1, Records Management Procedures, March 24, 2010
36. NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, June 10, 2014
37. NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015
38. OMB Memorandum, "Transition to IPv6", September 28, 2010
39. VA Directive 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, October 26, 2015
40. VA Handbook 0735, Homeland Security Presidential Directive 12 (HSPD-12) Program, March 24, 2014

41. OMB Memorandum M-06-18, Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006
42. OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
43. OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
44. OMB memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
45. OMB Memorandum, Guidance for Homeland Security Presidential Directive (HSPD) 12 Implementation, May 23, 2008
46. Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011
47. NIST SP 800-116, A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008
48. OMB Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007
49. NIST SP 800-63-3, 800-63A, 800-63B, 800-63C, Digital Identity Guidelines, June 2017
50. NIST SP 800-157, Guidelines for Derived PIV Credentials, December 2014
51. NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012
52. Draft National Institute of Standards and Technology Interagency Report (NISTIR) 7981 Mobile, PIV, and Authentication, March 2014
53. VA Memorandum, VAIQ #7100147, Continued Implementation of Homeland Security Presidential Directive 12 (HSPD-12), April 29, 2011 (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
54. IAM Identity Management Business Requirements Guidance document, May 2013, (reference Enterprise Architecture Section, PIV/IAM (reference https://www.voa.va.gov/documentlistpublic.aspx?NodeID=514)
55. VA Memorandum "Mandate to meet PIV Requirements for New and Existing Systems" (VAIQ# 7712300), June 30, 2015, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846
56. Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0, Federal Interagency Technical Reference Architectures, Department of Homeland Security, October 1, 2013, https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf
57. OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC), November 20, 2007
58. OMB Memorandum M-08-23, Securing the Federal Government's Domain Name System Infrastructure, August 22, 2008
59. VA Memorandum, VAIQ #7497987, Compliance – Electronic Product Environmental Assessment Tool (EPEAT) – IT Electronic Equipment, August 11, 2014 (reference Document Libraries, EPEAT/Green Purchasing Section, https://www.voa.va.gov/documentlistpublic.aspx?NodeID=552)
60. Sections 524 and 525 of the Energy Independence and Security Act of 2007, (Public Law 110–140), December 19, 2007
61. Section 104 of the Energy Policy Act of 2005, (Public Law 109–58), August 8, 2005
62. Executive Order 13693, "Planning for Federal Sustainability in the Next Decade", dated March 19, 2015
63. Executive Order 13221, "Energy-Efficient Standby Power Devices," August 2, 2001
64. VA Directive 0058, "VA Green Purchasing Program", July 19, 2013
65. VA Handbook 0058, "VA Green Purchasing Program", July 19, 2013

66. Office of Information Security (OIS) VAIQ #7424808 Memorandum, "Remote Access", January 15, 2014, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
67. Clinger-Cohen Act of 1996, 40 U.S.C. §11101 and §11103
68. VA Memorandum, "Implementation of Federal Personal Identity Verification (PIV) Credentials for Federal and Contractor Access to VA IT Systems", (VAIQ# 7614373) July 9, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
69. VA Memorandum "Mandatory Use of PIV Multifactor Authentication to VA Information System" (VAIQ# 7613595), June 30, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
70. VA Memorandum "Mandatory Use of PIV Multifactor Authentication for Users with Elevated Privileges" (VAIQ# 7613597), June 30, 2015; https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
71. "Veteran Focused Integration Process (VIP) Guide 2.0", May 2017, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371
72. "VIP Release Process Guide", Version 1.4, May 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4411
73. "POLARIS User Guide", Version 1.2, February 2016, https://www.voa.va.gov/DocumentView.aspx?DocumentID=4412
74. VA Memorandum "Use of Personal Email (VAIQ #7581492)", April 24, 2015, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28
75. VA Memorandum "Updated VA Information Security Rules of Behavior (VAIQ #7823189)", September, 15, 2017, https://www.voa.va.gov/DocumentListPublic.aspx?NodeId=28

3.0 SCOPE OF WORK

The Contractor shall provide VTP VetRide Subscription services to include maintenance, support, and equipment refresh of VTP VetRide. The Contractor shall serve as the single point of contact for all elements of VetRide to include Mobile Data Computers (MDC) refresh and installation, necessary telecom (voice, data & satellite plans) services, and other integration services as required for the VetRide.

4.0 PERFORMANCE DETAILS

4.1 PERFORMANCE PERIOD

The period of performance (PoP) shall be September 9, 2018 through March 8, 2019, followed by two 6-month option periods (if exercised).

Period of Performance		
Base	9/9/2018	3/8/2019
Option 1	3/9/2019	9/8/2019
Option 2	9/9/2019	3/8/2020

Any work at the Government site shall not take place on Federal holidays or weekends unless directed by the Contracting Officer (CO). If required, the CO may designate the Contractor to work during holidays and weekends.

There are ten (10) Federal holidays set by law (USC Title 5 Section 6103) that VA follows:

Under current definitions, four are set by date:

New Year's Day	January 1
Independence Day	July 4
Veterans Day	November 11
Christmas Day	December 25

If any of the above falls on a Saturday, then Friday shall be observed as a holiday. Similarly, if one falls on a Sunday, then Monday shall be observed as a holiday.

The other six are set by a day of the week and month:

Martin Luther King's Birthday	Third Monday in January
Washington's Birthday	Third Monday in February
Memorial Day	Last Monday in May
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Thanksgiving	Fourth Thursday in November

4.2 PLACE OF PERFORMANCE

Performance will be at the Contractor’s facility, except when a face to face status or planning meeting is necessary or requested. Work at the Government site shall not take place on federal holidays or weekends unless directed by the contracting officer.

4.3 TRAVEL

The Government anticipates travel under this effort to perform the tasks associated with the effort, as well as to attend program-related meetings or conferences throughout the PoP. Include all estimated travel costs in your firm-fixed-price line items. These costs will not be directly reimbursed by the Government.

The total estimated number of trips in support of the program for this effort is Thirty (30, 10 for base and each option period) trips for MDC installation and implementation of the VetRide. Location for status planning meetings will be determined by the Program Office. Anticipated locations could be any VAMC location not currently participating in the VTP program estimated at four (4) days per trip in duration. For estimation of the ten (10) trips per period please estimate at 12 MDC units per site and four (4) days per trip to include training:

Contract Year	# Trips	Duration/Trip
Base	10	4
Option 1	10	4
Option 2	10	4

Travel shall be in accordance with the Federal Travel Regulations (FTR) and requires advanced concurrence by the COR. Contractor travel within the local commuting area will not be reimbursed.

5.0 SPECIFIC TASKS AND DELIVERABLES

The Contractor shall preform the following:

5.1 PROJECT MANAGEMENT

5.1.1 CONTRACTOR PROJECT MANAGEMENT PLAN

The Contractor shall deliver a Contractor Project Management Plan (CPMP) that lays out the Contractor's approach, timeline and tools to be used in execution of the contract. The CPMP should take the form of both a narrative and graphic format that displays the schedule, milestones, risks and resource support. The CPMP shall also include how the Contractor shall coordinate and execute planned, routine, and ad hoc data collection reporting requests as identified within the PWS. The initial baseline CPMP shall be concurred upon and updated as needed. The Contractor shall update and maintain the VA PM approved CPMP throughout the PoP.

Deliverable:

A. Contractor Project Management Plan

5.1.2 KICK-OFF MEETING

The Contractor shall hold a technical kickoff meeting within 5 days after contract award. The Contractor shall present, for review and approval by the Government, the details of the approach, work plan, deliverables and project schedule for each effort. The Contractor shall specify dates, locations. The Contractor shall invite the Contracting Officer (CO), Contract Specialist (CS), COR, and the VA PM.

Deliverables:

A. Kickoff Meeting. Agenda

B. Kickoff Meeting Minutes

5.1.3 WEEKLY PROGRESS REPORT

The Contractor shall provide a weekly progress report in electronic form i.e. Microsoft Word and meet with the Program Office weekly to discuss VetRide task status activity, progress and cost management reports within 10 business days of award. The report shall include detailed instructions/explanations for any issues, to ensure that the software is working appropriately and issues are being addressed. These reports shall reflect data as of the last day of the preceding week.

The weekly Progress Reports shall cover all work completed during the reporting period and work planned for the subsequent reporting period. The report shall also continue also to identify any problems that arose and a description of how the problems were resolved. If problems have not been completely resolved, the Contractor shall provide an explanation including their plan and timeframe for resolving the issue. It is expected that the Contractor will keep in communication with VA accordingly so that issues that arise are transparent to both parties to prevent escalation of outstanding issues.

Dates and times for weekly meetings will be agreed upon during the kickoff meeting.

Deliverable:

A. Weekly Progress Report

5.1.4 DOCUMENTATION UPDATES

Contractor shall review all documentation at the end of each the base period and each option period (if exercised). The Contractor shall review and update all of the documentation including, but not limited to the following documents: PIA, System Security Plan, and Contingency Plan.

5.2 VETRIDE SCHEDULING SOFTWARE SYSTEM

The Contractor shall provide VetRide scheduling software system on a license subscription basis. The VetRide Scheduling Software System shall include the functionality identified in subparagraphs 5.2 through 5.11 including installation, deployment and operational maintenance with an operational availability of at least 96% during core hours of operation (Monday through Sunday from 5:30 AM – 12:00 AM (EST).

5.2.1 SYSTEM RESPONSE TIME

VetRide shall have an average screen latency time of 1 second not to exceed 3 seconds in more than 0.1% of cases.

VetRide shall not exceed a lag time of 3 seconds for more than 0.1% of the time in a rolling 12-month period.

5.2.2 CONCURRENT USERS

VetRide shall enable multiple transportation coordinators and other users (e.g., systems administrators) to access server software across multiple VAMC's without degradation of performance. VetRide shall be capable of tracking and communicating with multiple vehicles simultaneously deployed across multiple VAMC regions.

The VetRide scheduling and routing software shall support not less than 1,140 concurrent users. This is a rough approximation based on average of 7.5 users/drivers per site times the final number of sites (152). Final numbers are TBD.

5.2.3 ONSITE INSTALLATION SERVICES

The Contractor shall provide migration support of existing data for sites that are new to the VTP Program upon implementation of the VetRide.

5.2.4 ROUTING CAPABILITIES

VetRide provides interactive routing and re-routing planning for vehicles which has the ability to calculate a large distance matrix, up to 500x500 way points, for route planning and optimization. The Contractor shall provide interactive multiple vehicle route planning capability based on time and location clustering of rides. Interactive route planner shall continuously optimize the routes as user adds or deletes ride requests from the planner in order to increase productivity of the staff, allow ability to lock waypoints of a route. The real-time optimization shall not re-optimize visiting sequence of locked waypoints and shall ensure suitability of vehicle for a ride based on requested resources and vehicle's resources. VetRide enables real-time communication of routing information to dispatched drivers.

The Contractor VetRide subscription service shall support and maintain the following routing capabilities:

5.2.4.1 AUTOMATED ROUTING

The Contractor shall maintain automated interactive routing which automatically calculates routes for multiple vehicles and drivers and dispatches based on current traffic conditions, Veteran location, destination, wait time, travel time, load time, vehicle availability, driver availability, vehicle resources, current location when en route, and appointment time of the Veteran(s) being transported.

5.2.4.2 MANUAL ROUTING

The VetRide currently enables VTP staff to override auto-scheduling and manually modify routes by providing or locking waypoints or "legs" of a trip. Real-time optimization does not re-optimize visiting sequence of locked waypoints and ensures suitability of vehicle for a ride based on requested resources and vehicle resources.

5.2.4.3 ROUTING AND BEST ORDER

The VetRide currently provides best order and routing instructions based current traffic conditions, Veteran location, destination, wait time, travel time, load time, and appointment time of the Veteran being transported

5.2.4.4 DRIVER NAVIGATIONAL DIRECTIONS

The VetRide currently communicates in real-time navigational turn by turn directions and navigation in offline mode.

5.2.4.5 REAL-TIME AUTOMATED RE-ROUTING

The VetRide currently allows real-time automated re-routing of van and driver based on new or removed Veteran Destination To and/or Veteran Destination from entries. The automated rerouting feature shall allow for manual updates and changes to propose schedules utilizing an interactive user interface which shall be immediately followed by a re-optimized route and visual display for user final approval. The routing schedule built by the auto-scheduling optimizer shall display pickup time, drop-off time, appointment time, and wait time for each Veteran being transported.

5.2.4.6 RIDE ROUTE SCHEDULE UPDATES

The VetRide currently updates ride route schedules in real-time based on traffic delays, weather, or other variables identified during the ride. These updates then trigger passenger alerts utilizing the customized rules engine and notifications.

5.2.4.7 ROUTE OPTIMIZATION

The VetRide currently automates optimized route scheduling for each vehicle and driver to minimize distance, increase efficiency, and reduce costs while maximizing the vehicle and driver utilization thereby reducing Veteran wait and transport times. Each VAMC can configure optimization parameters allowing sites to customize requirements and build a schedule with or without preferred driver/vehicle pairings.

5.3 ADMINISTRATIVE PORTAL

The Contractor shall provide an Administrative Portal which contains a "single pane of glass" using integrated software codes and source code to integrate information from multiple sources into a unified display. The Contractor shall maintain an embedded user manual within the administrative portal which shall include a .pdf download for offline reading, the ability to view training videos, automated cost avoidance for Beneficiary Travel Special Mode of Transportation (SMT), i.e., wheelchair transport, Basic Life Support (BLS), stretcher, and Advanced Life Support (ALS). The Contractor shall provide the ability to schedule recurring runs on a weekly basis, Optimization of routes, identification of appropriate vehicle based on modality, track vehicles in real time via live map, replay run events using a replay runs page, optimization versus actual route taken, and the ability to enable multiple VetRide administrators across multiple VAMC's without degradation of performance.

The Contractor shall also provide the following functionality as part of the Administrative Portal:

5.3.1 ACCESS CONTROL, AUTHORIZATION, AND FACILITY MANAGEMENT

The VetRide currently provides support for multiple concurrent station users. The station users will function as VTP staff, will be able to receive requests for scheduled rides, will plan routes for vehicles/drivers, and will track/oversee dispatched vehicles. The current VetRide also requires custom entry of station capability which allows for entry of clinics and care provided on a customized station by station basis and allows for reporting of frequently used clinics by Veterans utilizing transportation.

The Contractor shall continue the current VetRide capability to provide for authentication of VA employees using the Personal Identity Verification (PIV) card. VetRide shall meet requirements outlined in NIST 800-53 security controls and VA 6500 information security handbook and provide a mutli-tenancy architecture where all VA sites can have their own operation autonomy. Each autonomous site shall have multi-tenancy architectural capability. A hierarchical access control shall be maintained so that each site operation can be managed by a Mobility Manger, VISN VTP Manager, Regional Coordinator, and all regions can be managed at a national level by Information Systems Administrators. Roles and permissions based on access control of VetRide data objects and functions shall be maintained as well as the ability to share data objects between autonomous sites as desired and configured by VA.

Role	Internal or External	Sensitivity Level	Authorized Privileges and Functions Performed
Information System Administrator	Internal	High	Site creation and management. Creates and manages all Internal accounts. All other system privileges listed.
Regional Coordinator	Internal	Moderate	Manage multiple sites. Enters traveler name, phone number address, travel/appointment schedule into VetRide.
VISN VTP Manager	Internal	Moderate	Manage multiple sites. Access to reports for multiple sites
Mobility Manager	Internal	Moderate	Manage site users account. Enters traveler name, phone number address, travel/appointment schedule into VetRide. Track vehicles. Dispatch drive schedule. Requests trips on behalf of users.
Transportation Coordinator	Internal	Moderate	Enters traveler name, phone number address, travel/appointment schedule into VetRide. Track vehicles. Dispatch drive schedule. Requests trips on behalf of users.
Driver	Internal	Moderate	Receives traveler name, phone number address, travel/appointment schedule from VetRide.
Reporting	Internal	Moderate	Access to required reports only.

5.3.2 SCHEDULING

VetRide shall continue to allow VTP administrative users to schedule Veterans trips through the Administrative Portal. The users will be able to schedule the trips to runs for either door to door or fixed routes. VetRide will also allow the users to schedule trips to runs that are already in progress.

5.3.2.1 APPOINTMENT TIME

VetRide shall continue to allow for Veteran appointment time to be entered and VetRide will calculate route and pick-up time with site adjustable parameters.

5.3.2.2 REOCCURRING RUNS

VetRide shall continue to allow for recurring pick-up and/or delivery orders to be entered without making a new entry.

5.3.2.3 DISPLAY VETERAN ACTIVE PICK-UP ORDERS

VetRide shall continue to display any active orders for pick-up or delivery once Veteran identification has been entered to ensure duplicate orders are not entered.

5.3.2.4 IDENTIFY CAREGIVER (COMPANION) SUPPORT

VetRide shall continue to identify if the passenger requires caregiver (companion). Veterans will be allowed to bring caregivers if they are determined to medically require such support.

5.3.2.5 ENTER SPECIAL PASSENGER INSTRUCTIONS

The Contractor shall maintain the ability to enable transportation coordinators to enter special instructions for drivers and/or VA attendants for specific passenger pick-ups and/or drop offs. Special instructions will include service dogs/animals, wheelchair, medical caregiver/companion, hearing impaired.

5.3.2.6 VETRIDE PASSENGER PICK-UP AND DESTINATION STORAGE

The Contractor shall maintain the database that allows for repeat addresses which can be verified for pick-up or drop-off.

5.3.2.7 ROUTE COST ANALYSIS

VetRide shall continue to provide the ability to calculate and analyze the cost of a route to determine the most economic routing for a specific passenger. This will need to include costs based on mileage (e.g. number of miles traveled multiplied by cost of gas per gallon) and third-party contract carrier costs.

5.3.2.8 AUTO-SCHEDULING/OPTIMIZATION

The Contractor shall continue to maintain the automatic ride scheduling feature. The Auto-Scheduling feature shall schedule Veterans' rides in a vehicle that can support the resources requested for that trip, create optimized route scheduling for each vehicle and driver to minimize distance, increase efficiency, and reduce costs while maximizing the vehicle and driver utilization thereby reducing Veteran wait and transport times. When determining optimized routes, the auto-scheduling feature shall consider driver and vehicle availability, shall stay within time restrictions, consider vehicle resources, capacity, allow a visual routing plan built for each driver and vehicle, the ability to configure optimization parameters allowing sites to customize requirements, and build a schedule with or without preferred driver/vehicle pairings.

The auto-scheduling feature shall allow for manual updates and changes to proposed schedules utilizing an interactive user interface which shall be immediately followed by a re-optimized route and visual display for user final approval. The routing schedule built by the auto-scheduling optimizer shall display pickup time, drop-off time, appointment time, and wait time for each Veteran being transported.

5.3.2.9 AUTOMATED VEHICLE LOG (AVL) PLAYBACK

VetRide shall maintain the ability for the transportation coordinator to playback the vehicle’s log on the map.

5.3.2.10 ADDRESS CORRECTION AND VALIDATION

VetRide shall continue to enable the transportation coordinator to correct and update an address to the actual map location (e.g. GeoCoded).

5.3.2.11 PASSENGER PRIORITIZATION BY NEED

VetRide shall maintain the ability to take into account the passengers’ special needs to manage vehicle capacity. This would ensure that Veterans with special needs are given top priority when being assigned to a vehicle.

5.3.2.12 WAIT LISTING RIDE REQUEST

VetRide shall continue to enable transportation coordinators to place Veterans requesting a ride on a prioritized wait list when rides are not available.

5.3.2.13 POINTS OF INTEREST (POI)

VetRide shall continue to allow the VetRide Administrative Portal users to enter Points of Interest to include the address, phone number, common name, and the Geo-Coded location.

5.3.2.14 RUN TEMPLATES

VetRide shall continue to allow the VetRide Administrative Portal users to create run templates. The run templates are routes for drivers that are generally recurring throughout a period of time. The run templates shall be searchable and editable. They must contain the name of the run template, where the run starts, and where the run ends at a minimum.

5.3.2.15 FACILITY CLOSURES

The Contractor shall maintain the ability of VetRide Administrative Portal users to create facility closure dates within the VetRide. If a closure date is created it will not allow any staff to schedule any trips for that day in the VetRide. The closure dates shall be searchable and filterable by date.

5.3.2.16 WALK-ON CAPABILITY

VetRide shall continue to allow for the drivers to create a walk on account for any Veteran that is not scheduled within the VetRide. The drivers shall be able to either manually create the passenger information or they will be able to swipe the Veterans identification Card (VIC). Once the walk on information is created it shall be sent to the VetRide Administrative Portal so that the VTP staff can create a new profile or merge the Veteran’s profile if one already exists.

5.3.3 FACILITY MANAGEMENT

The Contractor shall maintain the Facility Management features within the current VetRide. VTP staff shall continue to be able to review their site setting, make edits as needed to ensure facility profile and capabilities are correct.

5.3.3.1 CLINIC CREATION

The Contractor shall maintain the clinic creation feature within the facility profile management feature. Clinic identification includes clinic name and all relevant Stop Code documentation and allows the facility staff the ability to edit Stop Codes with respective changes of associated care. The Contractor shall also maintain the ability to select multiple clinics in the event that a Veteran has more than one appointment

5.3.3.2 ZONE CREATION AND MANAGEMENT

The Contractor shall maintain the zone creation and management capability which enables the Transportation Coordinator and Mobility Manager to create unique boundaries on the map as "zones".

5.3.3.3 OFFICE OF RURAL HEALTH (ORH) METRICS AND ANALYTICS TOOL (OMAT)

The Contractor shall ensure users are able to continue to enter and edit the OMAT identification number for sites with a rurality of 50% or greater so ORH may monitor and report metrics for facilities they support through the VTP partnership.

5.3.4 DRIVER AND VEHICLE MANAGEMENT

The Contractor shall maintain driver and vehicle management features within VetRide. The driver and vehicle management feature allows for the Transportation Coordinator and/or Mobility Manager to dispatch trips by showing vehicle availability, driver availability, resources, and vehicle capability to meet patient needs.

5.3.4.1 DRIVER AVAILABILITY

The Contractor shall maintain the ability to update the driver profile. The driver availability is driven by entering the drivers tour of duty as well as marking the driver as unavailable when on leave or when absent.

5.3.4.2 VEHICLE PROFILE AND AVAILABILITY

The Vehicle Availability functionality provides the capability to monitor if a vehicle is available based on its resources, capability to meet special needs, and capacity. This feature is used for scheduling trips manually and through the optimization/auto-scheduling feature.

5.3.4.3 VEHICLE POOLS

The Contractor shall maintain the ability to assign vehicles to a "pool." Vehicles included in this pool shall have specific vehicle capability to meet special needs of patients and will have an associated vehicle maintenance section tethered to their profile.

5.3.4.4 VEHICLE SERVICE LOGS

VetRide shall maintain the ability for staff to enter vehicle service logs anytime that the vehicle has any maintenance completed on it. These logs shall be able to be entered through the MDC device by the drivers or through the Administrative Portal by appropriate staff. VetRide shall collect the following data, at a minimum: date of the transaction; type of transaction; amount of the transaction; driver of the vehicle; and location where the service was completed. VetRide shall also do an average cost of maintenance per mile, fuel cost per mile, and miles per gallon. All data shall be searchable and filterable.

5.3.5 SPECIAL MODE OF TRANSPORTATION (SMT) TRACKER

The Contractor shall maintain the SMT tracker which shall track all rides and costs related to special mode transport (wheel chair, ALS, BLS, Stretcher), the Beneficiary Travel (BT) Eligibility and upcoming expiration of eligibility with weekly reminders beginning at four weeks out, and those that are assigned to third party service providers. VetRide shall automate the calculation process of transport cost related to SMT and provide cost avoidance metrics when such rides are picked up by the local VTS program instead of being referred to a third party provider. The SMT tracker shall be able to identify and flag an incorrect assignment of SMT based on the vendor's capability and or VTS vehicle capability, provide invoice management workflow from submission to payment. Invoices submitted through the SMT Tracker shall be reconciled by the

VetRide and include an audit trail of changes made to invoices and partial payments during the invoice lifecycle.

5.3.6 THIRD PARTY CONTRACT MANAGEMENT

Contractor shall maintain the Third Party Contract Management capability which allows sites to manage their third party contracts and contract vendors, share ride referrals with third party vendors through the VetRide Third Party Portal (VTPP) when a ride is referred to a contracted vendor, notify the Mobility Manager and Transportation Coordinator if referral is declined, accepted, completed etc. The Third Party Contract Management feature shall calculate costs of all third party assigned rides based on each contract cost model and establish between VTS and third party vendor and display the most cost efficient vendor for rides referred to third party service providers. Vendors shall be notified when a request for transport is made via email, text, and/or robo-call.

5.3.7 RULE ENGINE AND NOTIFICATION

The Contractor shall maintain the rules engine which allows for the building of custom rules for triggering of notifications. The rules engine shall provide the ability to send notifications by email, SMS, and phone call when important information needs to be communicated with the Veteran, VAMC, and/or Third party. The rule engine shall allow the VTP staff and VAMC, to define site-specific rules which respond to user-triggered as well as transient events involving in-vehicle actions performed by drivers, Veteran/passenger actions, third party actions, changes to trips, configure rule specific response actions which can include email, SMS, and robo-call, specify audience such as user or specific user role which can be defined on a site-by-site basis.

5.3.7.1 THRESHOLD MANAGEMENT AND WARNINGS

VetRide shall provide the ability to set thresholds to values (e.g. cost and “Special Mode”) and warn the user of possible threshold violations. For example, VetRide should warn/remind the user of the cost of “Special Mode” transportation versus VTS prior to scheduling a trip.

5.4 VETRIDE THIRD PARTY PORTAL (VTPP)

The Contractor shall maintain a separate third party portal for external vendors to manage trips that have been referred to them by site administrators, i.e., Mobility Managers and Transportation Coordinators. The VTPP shall require three pieces of information in order to register the third party vendor with the system. VetRide shall provide a workflow that allows third party vendors to search through their historical and upcoming trip requests as well the acceptance or rejection of referrals which notifies the VA Facility of a change in status. Third party vendors shall be able to enter and update trips to include costs, status, and comments. The VTPP shall be capable of storing a minimum of 10TB of special mode eligibilities and invoices with encryption at rest and in transit.

5.5 VETERAN SELF-SERVICE PORTAL (VSSP)

The Contractor shall maintain the current VSSP for Veterans to create an account, manage their ride requests which require approval workflow via the Administrative Portal, update profiles, verify status of trips, and cancel rides. VSSP shall provide Veterans the ability to create recurring trips on weekly and monthly recurrence a minimum of three months into the future. Ride requests made through the VSSP shall be validated by site administrative team members, i.e., Mobility Manager and Transportation Coordinator prior to its scheduling. VSSP shall be 508 certified by the VA 508 Compliance and Certification Team. VetRide shall meet requirements outlined in NIST 800-53 security controls and VA 6500 information security handbook. The VSSP shall provide Veteran and VA Facility notification via robo-call, text, and/or email based on VA Facility and Veteran preference.

5.6 MOBILE DATA COMPUTER (MDC) AND HARDWARE

The Contractor shall maintain Mobile Data Computers (MDC) designed to operate in outdoor or harsh environments for fleet management and passenger transport. Each unit must provide a continuous connection with VetRide utilizing dual mode satellite and cellular communication.

5.6.1 MDC HARDWARE REQUIREMENTS

The Contractor shall continue to maintain and update as required current software capable of Contractor's currently installed utilizing dual mode satellite and cellular communication hardware as well as MDC devices provided to the sites by the Contractor. Charges for all communication services incurred by dual mode communication as well as all equipment required for installation shall be included in the firm-fixed-price. Installation of units shall be done in a manner to prevent the unit from becoming a moving projectile in the event of an accident.

The Contractor shall install MDC's upon implementation of the VetRide at each new facility. The Contractor shall provide 70 units for the Base Period and each Option Period.

5.6.2 MDC SOFTWARE REQUIREMENTS

The Contractor shall provide software for the MDC units which will allow drivers to login using their VA Personal Identity Verification (PIV) card, have ability to receive schedule updates in real-time, ability to update new versions of applications, continuously update its map data, the ability to perform real-time navigation in offline mode, and provide the ability to read the Veterans Health Identification Cards (VHIC) assigned to Veterans for verification of the ridership (loading, unloading, load time).

The MDC software shall enable the MDC to communicate in real-time; navigation in offline mode, all passenger loading/unloading events, bi-directional messaging between MDC and Administrative Portal users, notify all vehicle location changes, provide traffic and weather conditions, monitor and warn drivers of speeding violations, and have ability to track all vehicle resources consumed by walk-on veterans. MDC's shall also serve as "dumb clients" that will not store information on the devices. MDC's shall also provide accurate odometer tracking, fuel and maintenance log tracking.

5.6.3 MDC UNIT INSTALLATION

The Contractor shall install all MDC units issued to sites specified by the Contracting Officer's Representative. The Contractor shall provide all required equipment to complete the installation. There are currently 787 MDC units deployed with 469 of those units also having satellite receivers.

The Contractor shall provide Installation status in the Weekly Progress Report. Upon completion of MDC Unit Refresh and Installation, the Contractor shall obtain Mobility Manager or designee signature validating successful completion of work.

Deliverable:

A. Mobility Manager or designee signed validation of work completed

5.6.4 FAILURE RATE

Failure rate of component systems should be less than .5% in a rolling 12-month period.

5.7 SYSTEM HOSTING

VetRide shall continue to be hosted and maintained within the Contractor's VA FedRAMP compliant cloud with auto scalability to cope with increased system load. The Contractor shall ensure synchronized multiple availability zones to protect against single site outage and shall manage and provision its infrastructure using infrastructure source code. The Contractor shall maintain zero downtime deployment methods to avoid disruption of service during software maintenance and updates. The Contractor shall maintain infrastructure as code and shall continue to support the ability to perform rollbacks of application deployment sequence without affecting the systems accessibility. The Contractor shall maintain and service standby equipment to prevent failover without downtime when the system fails. The Contractor shall maintain the "single pane of glass" using integrated software codes and source code to integrate information from multiple sources into a unified display.

During the period of performance (base or option periods) the Government may migrate from a Contractor hosted VetRide to the VA Enterprise Cloud (VAEC). In the event that the Government determines migration to VAEC is required, the Contractor shall facilitate a VetRide Migration Planning meeting to coordinate the support required between VAEC Office and the Contractor to migrate the VetRide to the VAEC. The Government will provide the Contractor with access to the VAEC to include the credits required for all Software as a Service (SaaS) cloud subscription service, testing and production environment requirements. The VAEC will also include a secure dedicated Wide Area Network connection between VA and the VAEC Cloud Service Provider (CSP) AWS. The VAEC AWS is currently supported by FedRAMP High Certified and VA Authority to Operate approved. In addition, VAEC provides a set of common shared services such as security scanning, Active Directory and single sign-on (SSO), PIV integration and performance monitoring to facilitate solution implementation. Specifications for the VAEC CSP, including access requirements, will be provided at the VetRide Migration Planning meeting.

5.8 DATA COLLECTION AND REPORTING

5.8.1 DATA WAREHOUSE

VetRide shall continue to provide the ability to generate reports that provide an insight into the performance of customer sites and shall convert production data into a format for efficient report generation and store it in a separate isolated warehousing database. The importation of data into the warehouse database shall occur between 11:00PM and 4:00AM EST to prevent a negative impact by the generation of reports. Data shall be presented in a generic format so that it may be displayed in both the browser as well as an Excel workbook. VetRide shall provide the ability to visualize report data using various graphs within the web browser application in line, pie, column, and bar formats.

5.8.2 CANNED REPORTS

The Contractor shall maintain the following canned reports:

a. All Totals
b. Trip Totals
c. Run Totals
d. Beneficiary Travel Cost Avoidance Totals
e. Passengers
f. Unique Passengers
g. Clinic Attendance

h. Clinic Attendance by Site
i. Beneficiary Travel Mileage Avoidance
j. Beneficiary Travel SMT Cost Savings
k. Trips by State
l. Trips by City
m. Trips by Zip Code
n. Blind Rehab
o. Third Party
p. Trip Denial
q. Vehicle Log
r. Status Report
s. Weekly Compliance Report

5.8.3 OFFICE OF RURAL HEALTH (ORH) REPORTING

The Contractor shall maintain the current ORH reporting capability utilizing the OMAT ID.

5.8.4 INFORMATION REPOSITORY

The Contractor shall ensure that VetRide provides the capability to enter and update information about drivers, vehicles, devices, passengers, attendants, and trips. The Contractor shall also ensure VetRide is flexible to accommodate new user-defined fields and constraint values as requested by the COR.

VetRide shall provide the ability to enter, the following information:

5.8.4.1 PASSENGER INFORMATION

a. Passenger Name (Last Name, First Name)
b. Passenger Gender
c. Passenger Home Address (Including County)
d. Passenger Mailing Address
e. Passenger Currently Active
f. Pick up and drop off date and time
g. Appointment date and time
h. Unique Veteran ID encoded on the Veteran ID card
i. Passenger Contact Information:
    - Home Phone
    - Mobile Phone
    - Other Phone (and Type)
    - e-Mail Address
j. Passenger Contact Preference
k. Passenger Type: Veteran, Veteran Companion
l. Mobility Type
m. Wheelchair Need: Yes/No identifier
n. Load Times (average time for passengers to get on and off vehicle)
o. Other Special Needs of Veteran:
    - Ambulatory
    - Blind/Site Impaired
    - Hearing Impaired
    - Service Animal
p. Other Special Needs: This should allow the notes on special needs of the rider.
q. Affiliated Veteran: for Veteran caregiver, the software will be modified to ensure the attendant is associated with a specific Veteran. Veterans are allowed to have caregivers travel with them if it is determined that it is medically required.
r. Clinical Priority of Veteran (Should be able to select multiple clinics if necessary)
s. Eligibility for Special Mode

t. Eligibility for Beneficiary Travel (By Trip)
u. Funding source (Special Mode, VTS, etc.)
v. Ability to track additional information as needed (OEF/OIF, Homeless, Veterans Justice Outreach, Rural, Highly Rural, Urban, etc.)

5.8.4.2 VEHICLE INFORMATION

a. Vehicle ID
b. Vehicle Mileage
c. Vehicle Type, to include:
   - Ability to build different vehicle types (12 passenger van, Large Bus, Minivan, etc.)
d. Vehicle Pool o Voluntary Service
   - Fleet Vehicle
   - Contractor Vehicle
   - Ability to build different vehicle pool (Voluntary Service, Fleet Vehicle, etc.)
e. Vehicle Passenger Capacity
f. Vehicle Capabilities (Low Floors, Wheel Chair Lift)
g. Vehicle Custom Fields
   - Ability to create custom fields to track vehicle information (Fuel Type, Last Service Date, etc.)
h. Vehicle Availability: Y/N
i. Vehicle Characteristics
   - Ability to create different characteristics as needed
j. Vehicle Description
   - Make
   - Model
   - Color
   - Year
k. Vehicle In-Service/Out-of-Service Status
l. Vehicle Cost Tracking o Deprecation Tracker
   - Fuel Cost
   - Driver Cost

5.8.4.3 DRIVER INFORMATION

a. Driver’s Name
b. Address (Drivers or VA)
c. Driver’s Phone Number
d. Driver’s License Number
e. Driver’s Hire Date
f. Comment’s Section
g. Work Schedule
h. Emergency Contact Information
   - Name
   - Phone Number
   - Relationship
i. Drivers Characteristics
   - Air Brake Certified Y/N
   - Commercial Driver’s License Y/N
j. Custom Fields
   - Training
   - Physical
   - Certifications

5.8.4.4 DEVICE INFORMATION

a. GPS Device ID
b. Associate Vehicle ID (where device is deployed)

5.8.4.5 TRIP INFORMATION

a. Trip ID
b. Pickup Address
c. Drop-off Address
d. Service being used
e. Trip timing preference
   - Drop-off
   - Pickup
f. Trip date and time
g. Trip Status
h. Trip request pickup/drop-off time
i. Trip type
j. Cost for Trip (Ability to calculate the costs for different fare types)
   - Ability to track and formulate the Beneficiary Travel Cost Avoidance
   - Ability to track and formulate the Special Mode Cost Avoidance
k. Trip Fare Type
   - VTS
   - Special Mode
   - Beneficiary Travel
   - Contract
l. Trip Purpose
m. Clinic Being Visited (Ability to choose multiple clinics)
n. Trip Load time
o. Trip Unload time
p. Number of passengers per trip
q. Duration of trip
r. Distance for trip
s. Trip route

5.8.4.6 DATA ANALYSIS

VetRide shall continue to provide the ability to export data Information Repository data to external systems for analysis and reporting.

5.8.4.7 AUDIT LOGGING

VetRide shall continue to provide the ability to log addition and updates performed by the user on the Information Repository for audit purposes.

5.8.4.8 HISTORICAL LOGGING

VetRide shall continue to provide the ability to log historical changes of key data such as the trips undertaken by a particular passenger over time.

5.8.4.9 DATA VERIFICATION

VetRide shall continue to provide the ability to verify the trip information in the Information Repository against the information in the Mobile Data Computer. This type of validation is needed to ensure that “planned” vs. “actual” trip information can be reconciled.

5.8.4.10 ENTER AND DISPLAY VETERAN INFORMATION

VetRide shall maintain the ability of information for passenger (Veteran) data to be entered, stored, and managed.

5.9 HELPDESK SERVICES

The Contractor shall provide HelpDesk services on a 24/7 basis, provide tiered level defect resolution for VetRide using the Institute of Electronics and Electrical Engineering (IEEE) classification structure. The Contractor shall update the VTP VetRide handbook as required when changes are made.

Deliverable:

A. Updated VTP VetRide Handbook

5.10 TRAINING

The Contractor shall provide training upon initial stand up of the solution and receiving signed documentation of training by participating members, monthly training calls when requested by the Program Office, all MDC training, and training for approved enhancements. Individualized "one on one" site training outside of the criteria above will be provided by the Region's VTS Coordinator with escalation to the Contractor only when necessary. The Contractor shall provide a Daily Training Report for all on-site training. The Daily Training Report shall consist of arrival time, meeting with on-site personnel, a detail list of training provided by timeframe, the individual(s) trained, any applicable notes and agenda for following day.

For estimating purposes, VA estimates on site training should at approximately ten sites in each for the base period and option periods for up to 25 staff to be trained in each period.

Deliverable:

A. Daily Training Report

5.11 SATELLITE AND CELLULAR COMMUNICATION REQUIREMENTS

VetRide shall have the ability to maintain a communication link with all operating vehicles using a dual model transceiver supporting both satellite and cellular communication capabilities. Also, the VetRide shall seamlessly switch mode of communication with the vehicles as vehicles move in and out of cellular data coverage areas when a satellite receiver is required due to limited coverage areas.

Note: Satellite receivers are only required when needed due to cellular coverage limitations. The Program Office is the final determination for reception and installation of satellite receivers.

5.11.1 DRIVER DEVICE CONNECTIVITY AND UPTIME

VTS drivers (both employees and volunteers) will, at times, be dispatched to remote, rural settings. The Contractor shall ensure that driver navigation and communication devices maintain connectivity and, in the event of connectivity loss, that these devices rapidly restore communications.

In the event of loss of driver navigation equipment, the driver navigation equipment shall restore connectivity within 5 seconds of re-establishing cellular or satellite signal.

5.11.2 FAILURE RATE

Failure rate of component systems should be less than .5% in a rolling 12-month period.

6.0 GENERAL REQUIREMENTS

6.1 ENTERPRISE AND IT FRAMEWORK

6.1.1 ONE-VA TECHNICAL REFERENCE MODEL

The Contractor shall support the VA enterprise management framework. In association with the framework, the Contractor shall comply with OI&T Technical Reference Model (One-VA TRM). One-VA TRM is one component within the overall Enterprise Architecture (EA) that establishes a common vocabulary and structure for describing the information technology used to develop, operate, and maintain enterprise applications. One-VA TRM includes the Standards Profile and Product List that collectively serves as a VA technology roadmap. Architecture, Strategy, and Design (ASD) has overall responsibility for the One-VA TRM.

6.1.2 FEDERAL IDENTITY, CREDENTIAL, AND ACCESS MANAGEMENT (FICAM)

The Contractor shall ensure Commercial Off-The-Shelf (COTS) product(s), software configuration and customization, and/or new software are Personal Identity Verification (PIV) card-enabled by accepting HSPD-12 PIV credentials using VA Enterprise Technical Architecture (ETA), http://www.ea.oit.va.gov/VA_EA/VAEA_TechnicalArchitecture.asp, and VA Identity and Access Management (IAM) approved enterprise design and integration patterns, http://www.techstrategies.oit.va.gov/enterprise_dp.asp. The Contractor shall ensure all Contractor delivered applications and systems comply with the VA Identity, Credential, and Access Management policies and guidelines set forth in the VA Handbook 6510 and align with the Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance v2.0.

The Contractor shall ensure all Contractor delivered applications and systems provide user authentication services compliant with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, VA Handbook 6500 Appendix F, “VA System Security Controls”, and VA IAM enterprise requirements for direct, assertion based authentication, and/or trust based authentication, as determined by the design and integration patterns. Direct authentication at a minimum must include Public Key Infrastructure (PKI) based authentication supportive of PIV card and/or Common Access Card (CAC), as determined by the business need.

The Contractor shall ensure all Contractor delivered applications and systems conform to the specific Identity and Access Management PIV requirements set forth in the Office of Management and Budget (OMB) Memoranda M-04-04, M-05-24, M-11-11, and NIST Federal Information Processing Standard (FIPS) 201-2. OMB Memoranda M-04-04, M-05-24, and M-11-11 can be found at: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy04/m04-04.pdf, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf, and https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf respectively. Contractor delivered applications and systems shall be on the FIPS 201-2 Approved Product List (APL). If the Contractor delivered application and system is not on the APL, the Contractor shall be responsible for taking the application and system through the FIPS 201 Evaluation Program.

The Contractor shall ensure all Contractor delivered applications and systems support:

1. Automated provisioning and are able to use enterprise provisioning service.

2. Interfacing with VA's Master Veteran Index (MVI) to provision identity attributes, if the solution relies on VA user identities. MVI is the authoritative source for VA user identity data.
3. The VA defined unique identity (Secure Identifier [SEC ID] / Integrated Control Number [ICN]).
4. Multiple authenticators for a given identity and authenticators at every Authenticator Assurance Level (AAL) appropriate for the solution.
5. Identity proofing for each Identity Assurance Level (IAL) appropriate for the solution.
6. Federation for each Federation Assurance Level (FAL) appropriate for the solution, if applicable.
7. Two-factor authentication (2FA) through an applicable design pattern as outlined in VA Enterprise Design Patterns.
8. A Security Assertion Markup Language (SAML) implementation if the solution relies on assertion based authentication. Additional assertion implementations, besides the required SAML assertion, may be provided as long as they are compliant with NIST SP 800-63-3 guidelines.
9. Authentication/account binding based on trusted Hypertext Transfer Protocol (HTTP) headers if the solution relies on Trust based authentication.
10. Role Based Access Control.
11. Auditing and reporting capabilities.
12. Compliance with VAIQ# 7712300 Mandate to meet PIV requirements for new and existing systems. https://www.voa.va.gov/DocumentView.aspx?DocumentID=4846

The required Assurance Levels for this specific effort are Identity Assurance Level 3, Authenticator Assurance Level 3, and Federation Assurance Level 3.

6.1.3 INTERNET PROTOCOL VERSION 6 (IPV6)

The Contractor solution shall support the latest Internet Protocol Version 6 (IPv6) based upon the directives issued by the Office of Management and Budget (OMB) on August 2, 2005 (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-22.pdf) and September 28, 2010 (https://cio.gov/wp-content/uploads/downloads/2012/09/Transition-to-IPv6.pdf). IPv6 technology, in accordance with the USGv6 Profile, NIST Special Publication (SP) 500-267 (https://www.nist.gov/programs-projects/usgv6-technical-basis-next-generation-internet), the Technical Infrastructure for USGv6 Adoption (http://www-x.antd.nist.gov/usgv6/index.html), and the NIST SP 800 series applicable compliance (http://csrc.nist.gov/publications/PubsSPs.html) 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 shall support native IPv6 and/or 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 and/or dual stack (IPv6/ IPv4) users and all internal infrastructure and applications shall communicate using native IPv6 and/or dual stack (IPv6/ IPv4) operations. Guidance and support of improved methodologies which ensure operability with legacy protocol and services in dual stack solutions, in addition to OMB/VA memoranda, can be found at: https://www.voa.va.gov/documentlistpublic.aspx?NodeID=282.

6.1.4 TRUSTED INTERNET CONNECTION (TIC)

The Contractor solution shall meet the requirements outlined in Office of Management and Budget Memorandum M08-05 mandating Trusted Internet Connections (TIC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/

m08-05.pdf), M08-23 mandating Domain Name System Security (NSSEC) (https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf), and shall comply with the Trusted Internet Connections (TIC) Reference Architecture Document, Version 2.0 https://s3.amazonaws.com/sitesusa/wp-content/uploads/sites/482/2015/04/TIC_Ref_Arch_v2-0_2013.pdf.

6.1.5 STANDARD COMPUTER CONFIGURATION

The Contractor IT end user solution that is developed for use on standard VA computers shall be compatible with and be supported on the standard VA operating system, currently Windows 7 (64bit), Internet Explorer 11 and Microsoft Office 2010. In preparation for the future VA standard configuration update, end user solutions shall also be compatible with Office 365 ProPlus and Windows 10. However, Office 365 ProPlus and Windows 10 are not the VA standard yet and are currently approved for limited use during their rollout, we are in-process of this rollout and making them the standard by OI&T. Upon the release approval of Office 365 ProPlus and Windows 10 individually as the VA standard, Office 365 ProPlus and Windows 10 will supersede Office 2010 and Windows 7 respectively. Applications delivered to the VA and intended to be deployed to Windows 7 workstations shall be delivered as a signed .msi package with switches for silent and unattended installation and updates shall be delivered in signed .msp file formats for easy deployment using System Center Configuration Manager (SCCM) VA's current desktop application deployment tool. Signing of the software code shall be through a vendor provided certificate that is trusted by the VA using a code signing authority such as Verizon/Cybertrust or Symantec/VeriSign. The Contractor shall also ensure and certify that their solution functions as expected when used from a standard VA computer, with non-admin, standard user rights that have been configured using the United States Government Configuration Baseline (USGCB) and Defense Information Systems Agency (DISA) Secure Technical Implementation Guide (STIG) specific to the particular client operating system being used.

6.1.6 VETERAN FOCUSED INTEGRATION PROCESS (VIP)

The Contractor shall support VA efforts IAW the Veteran Focused Integration Process (VIP). VIP is a Lean-Agile framework that services the interest of Veterans through the efficient streamlining of activities that occur within the enterprise. The VIP Guide can be found at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4371. The VIP framework creates an environment delivering more frequent releases through a deeper application of Agile practices. In parallel with a single integrated release process, VIP will increase cross-organizational and business stakeholder engagement, provide greater visibility into projects, increase Agile adoption and institute a predictive delivery cadence. VIP is now the single authoritative process that IT projects must follow to ensure development and delivery of IT products

6.1.7 PROCESS ASSET LIBRARY (PAL)

The Contractor shall utilize PAL, the OI&T-wide process management tool that assists in the execution of an IT project (including adherence to VIP standards). PAL serves as an authoritative and informative repository of searchable processes, activities or tasks, roles, artifacts, tools and applicable standards or guides to assist project teams in facilitating their VIP compliant work.

6.2 SECURITY AND PRIVACY REQUIREMENTS

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

6.2.1 SECURITY & PRIVACY

Contractor shall maintain the systems capability to provide for authentication of VA employees using the Personal Identity Verification (PIV) card. The system shall meet requirements outlined in NIST 800-53 security controls and VA 6500 information security handbook and provide a mutli-tenancy architecture where all VA sites can have their own operation autonomy. Each autonomous site shall have multi-tenancy architectural capability. A hierarchical access control shall be maintained so that each site operation can be managed by a Regional Coordinator and all regions can be managed at a national level. Roles and permissions based on access control of the system's data objects and functions shall be maintained as well as the ability to share data objects between autonomous sites as desired and configured by VA.

The solution shall ensure that all Veteran information is secured and conforms to VA information security standards. VA is required to protect Personally Sensitive Information (SPI) in accordance with the latest version of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 and the VA Information Security Handbook 6500. A Risk Assessment should be conducted to determine the Security Category of the data, and then the appropriate security controls should be assigned as a baseline. These are the preliminary steps in the Assessment and Authorization (A&A) process, which is the process required to obtain an Authority to Operate (ATO). The VA will assist in A&A process, providing guidance and support to the vendor.

The Contractor shall be responsible for conducting the A&A, as providing proof to the VA of the results of the process so an ATO can be issued by the VA. Specific requirements for security Managed Services can be found in the document included below:

Department of Veterans Affairs
1615 Woodward St.
Austin Texas 78772

The Contractor shall maintain and ensure that their security postures, as well as all pertinent documentation are existent and up to date.

According to the Mandatory Security Requirements Contained in Informatiion Protectect And Risk Management (IPRM's) Statement of Objectives/Performance Work Statement" and VA Handbook 6500.6:

- Outsourcing (contractor facility, contractor equipment or contractor staff) of systems or network operations, telecommunications services, or other managed services requires Assessment & Authorization (A&A) of the contractor's systems in accordance with VA Handbook 6500.3, *Certification and Accreditation* and/or the VA OCS Certification Program Office. Government-owned (government facility or government equipment) contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.
- The contractor/subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA contracting officer and the ISO for entry into VA's POA&M management process. The contractor/subcontractor must use VA's POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures,

and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the government. Contractor/subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with contractor/subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the C&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, Contingency Plan). The Certification Program Office can provide guidance on whether a new C&A would be necessary.

- The contractor/subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COTR. The government reserves the right to conduct such an assessment using government personnel or another contractor/subcontractor. The Contractor/subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

Summary:

- The Security Control Assessment (SCA) will be completed by VA on an annual basis.
- The completed SCA will be reviewed by the ISO and by the Certification Program Office to ensure that adequate security is being addressed by contractors in situations where the C&A of a system is not applicable.
- The document repository for the Managed Services is kept in SMART.
- Any other supporting documentation provided by the Managed Service (i.e. SSP, Corporate Information Security Policy, Business Continuity Plan, Disaster Recovery Plan) will also be uploaded into SMART under the specific Managed Service.
- The Artifacts for Managed Services are uploaded directly into the “Document” section in SMART only

Any questions pertaining to the information above should be addressed to Charles Aponte, National Data Center Information Security Officer at (512) 981-4405 or by email Charles.aponte2@va.gov .

The current VetRide Solution and VA environment utilize the following:

- The use of SSL
- Passwords that follow the 6500 Standard
- Citrix Remote Client
- Devices that follow the FIPS (Federal Information Processing Standard) 140-2 for Field devices.

Refer to entitled “Federal Standards and Guidelines” for a comprehensive list of information privacy and security requirements.

6.2.1.1 POSITION/TASK RISK DESIGNATION LEVEL(S)

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

Position Sensitivity and Background Investigation Requirements by Task

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.1	☐	☒	☐

Task Number	Tier1 / Low Risk	Tier 2 / Moderate Risk	Tier 4 / High Risk
5.2	□	☒	□
5.3	□	☒	□
5.4	□	☒	□
5.5	□	☒	□
5.6	□	☒	□
5.7	□	☒	□
5.8	□	☒	□
5.9	□	☒	□
5.10	□	☒	□
5.11	□	☒	□

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.

6.2.1.2 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

Contractor 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.

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 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 are to encrypt the file, use a secure fax, or use a traceable mail service.

b. 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 Security and Investigations Center (SIC) Fingerprint request form with them (see paragraph d.4. below) when getting fingerprints taken.

c. 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 SIC Fingerprint Request Form

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 Office of Personnel Management's (OPM) Electronic Questionnaire for Investigations Processing (e-QIP) after receiving an email notification from the Security and Investigation Center (SIC).

The Contractor employee shall certify and release the e-QIP document, print and sign the signature pages, and send them encrypted to the COR for electronic submission to the SIC. These documents shall be submitted to the COR within 3 business days of receipt of the e-QIP notification email. (Note: OPM 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 e-QIP).

d. 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.

e. 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 9), signed "Contractor Rules of Behavior", and with a valid, operational 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 OPM. 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 OPM.

f. 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.

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.

Identity 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

6.3 METHOD AND DISTRIBUTION OF DELIVERABLES

The Contractor shall deliver documentation in electronic format, unless otherwise directed in Section B of the solicitation/contract. Acceptable electronic media include: MS Word 2000/2003/2007/2010, MS Excel 2000/2003/2007/2010, MS PowerPoint 2000/2003/2007/2010, MS Project 2000/2003/2007/2010, MS Access 2000/2003/2007/2010, MS Visio 2000/2002/2003/2007/2010, AutoCAD 2002/2004/2007/2010, and Adobe Postscript Data Format (PDF).

6.4 PERFORMANCE METRICS

The table below defines the Performance Standards and Acceptable Levels of Performance associated with this effort.

Performance Objective	Performance Standard	Acceptable Levels of Performance
A. Technical / Quality of Product or Service	1. Demonstrates understanding of requirements 2. Efficient and effective in meeting requirements 3. Meets technical needs and mission requirements 4. Provides quality services/products	Satisfactory or higher
A1. Availability	See requirement 5.2	In the event of loss of driver navigation equipment, the driver navigation equipment will restore connectivity within 5 seconds of restoring communications.
A2. Connectivity Uptime	See requirement 5.11.1	In the event of loss of driver navigation equipment, the driver navigation equipment will restore connectivity within 5 seconds of restoring communications.
A3 Failure Rates	See requirement 5.6.4 & 5.11.2	should be less than .5% in a rolling 12 month period
A4. System Response Time	See requirement 5.2.1	System shall have an average screen latency time of 1 second not to exceed 3 seconds in more than 0.1% of cases. System shall not exceed a lag time of 3 seconds for more than 0.1% of the time in a rolling 12 month period. System shall maintain an average lag time of less than 2 seconds 96% of the time in a rolling 12 month period. System shall maintain an average system response time of less than 2 seconds 96% of the time for a rolling 12 month period.

B. Project Milestones and Schedule	1. Established milestones and project dates are met 2. Products completed, reviewed, delivered in accordance with the established schedule 3. Notifies customer in advance of potential problems	Satisfactory or higher
C. Cost & Staffing	1. Currency of expertise and staffing levels appropriate 2. Personnel possess necessary knowledge, skills and abilities to perform tasks	Satisfactory or higher
D. Management	1. Integration and coordination of all activities to execute effort	Satisfactory or higher

The COR will utilize a Quality Assurance Surveillance Plan (QASP) throughout the life of the contract to ensure that the Contractor is performing the services required by this PWS in an acceptable level of performance. The Government reserves the right to alter or change the surveillance methods in the QASP at its own discretion. A Performance Based Service Assessment will be used by the COR in accordance with the QASP to assess Contractor performance.

6.5 FACILITY/RESOURCE PROVISIONS

The Government will provide office space, telephone service and system access when contract staff are authorized or required to work at a Government location as required in order to accomplish the Tasks associated with this PWS. All procedural guides, reference materials, and program documentation for the project and other Government applications will also be provided on an as-needed basis.

The Contractor shall request other Government documentation deemed pertinent to the work accomplishment directly from the Government officials with whom the Contractor has contact. The Contractor shall consider the COR as the final source for needed Government documentation when the Contractor fails to secure the documents by other means. The Contractor is expected to use common knowledge and resourcefulness in securing all other reference materials, standard industry publications, and related materials that are pertinent to the work.

VA may provide remote access to VA specific systems/network in accordance with VA Handbook 6500, which requires the use of a VA approved method to connect external equipment/systems to VA's network. Citrix Access Gateway (CAG) is the current and only VA approved method for remote access users when using or manipulating VA information for official VA Business. VA permits CAG remote access through approved Personally Owned Equipment (POE) and Other Equipment (OE) provided the equipment meets all applicable 6500 Handbook requirements for POE/OE. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved POE or OE. The Contractor shall provide proof to the COR for review and approval that their POE or OE meets the VA Handbook 6500 requirements and VA Handbook 6500.6 Appendix C, herein incorporated as Addendum B, before use. CAG authorized users shall not be permitted to copy, print or save any VA information accessed via CAG at any time. VA prohibits remote access to VA's network from non-North Atlantic Treaty Organization (NATO) countries. The exception to this are countries where VA has approved operations established (e.g. Philippines and South Korea). Exceptions are determined by the COR in coordination with the Information Security Officer (ISO) and Privacy Officer (PO).

This remote access may provide access to VA specific software such as Veterans Health Information System and Technology Architecture (VistA), ClearQuest, PAL, Primavera, and Remedy, including appropriate seat management and user licenses, depending upon the level of access granted. The Contractor shall utilize government-provided software development and test accounts, document and requirements repositories, etc. as required for the development, storage, maintenance and delivery of products within the scope of this effort. The Contractor shall not transmit, store or otherwise maintain sensitive data or products in Contractor systems (or media) within the VA firewall IAW VA Handbook 6500.6 dated March 12, 2010. All VA sensitive information shall be protected at all times in accordance with VA Handbook 6500, local security field office System Security Plans (SSP's) and Authority to Operate (ATO)'s for all systems/LAN's accessed while performing the tasks detailed in this PWS. The Contractor shall ensure all work is performed in countries deemed not to pose a significant security risk. For detailed Security and Privacy Requirements (additional requirements of the contract consolidated into an addendum for easy reference) refer to ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED and ADDENDUM B - VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE.

6.6 GOVERNMENT FURNISHED PROPERTY

Not Applicable

ADDENDUM A – ADDITIONAL VA REQUIREMENTS, CONSOLIDATED

A1.0 Cyber and Information Security Requirements for VA IT Services

The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. The Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation.

Contractor supplied equipment, PCs of all types, equipment with hard drives, etc. for contract services must meet all security requirements that apply to Government Furnished Equipment (GFE) and Government Owned Equipment (GOE). Security Requirements include: a) VA Approved Encryption Software must be installed on all laptops or mobile devices before placed into operation, b) Bluetooth equipped devices are prohibited within VA; Bluetooth must be permanently disabled or removed from the device, unless the connection uses FIPS 140-2 (or its successor) validated encryption, c) VA approved anti-virus and firewall software, d) Equipment must meet all VA sanitization requirements and procedures before disposal. The COR, CO, the PM, and the Information Security Officer (ISO) must be notified and verify all security requirements have been adhered to.

Each documented initiative under this contract incorporates VA Handbook 6500.6, "Contract Security," March 12, 2010 by reference as though fully set forth therein. The VA Handbook 6500.6, "Contract Security" shall also be included in every related agreement, contract or order. The VA Handbook 6500.6, Appendix C, is included in this document as Addendum B.

Training requirements: The Contractor shall complete all mandatory training courses on the current VA training site, the VA Talent Management System (TMS), and will be tracked therein. The TMS may be accessed at https://www.tms.va.gov. If you do not have a TMS profile, go to https://www.tms.va.gov and click on the "Create New User" link on the TMS to gain access.

Contractor employees shall complete a VA Systems Access Agreement if they are provided access privileges as an authorized user of the computer system of VA.

A2.0 VA Enterprise Architecture Compliance

The applications, supplies, and services furnished under this contract must comply with One-VA Enterprise Architecture (EA), available at http://www.ea.oit.va.gov/index.asp in force at the time of issuance of this contract, including the Program Management Plan and VA's rules, standards, and guidelines in the Technical Reference Model/Standards Profile (TRMSP). VA reserves the right to assess contract deliverables for EA compliance prior to acceptance.

VA Internet and Intranet Standards

The Contractor shall adhere to and comply with VA Directive 6102 and VA Handbook 6102, Internet/Intranet Services, including applicable amendments and changes, if the Contractor's work includes managing, maintaining, establishing and presenting information on VA's Internet/Intranet Service Sites. This pertains, but is not limited to: creating announcements; collecting information; databases to be accessed, graphics and links to external sites.

Internet/Intranet Services Directive 6102 is posted at (copy and paste the following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=409&FType=2

Internet/Intranet Services Handbook 6102 is posted at (copy and paste following URL to browser): http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=410&FType=2

A3.0 Notice of the Federal Accessibility Law Affecting All Electronic and Information Technology Procurements (Section 508)

On August 7, 1998, Section 508 of the Rehabilitation Act of 1973 was amended to require that when Federal departments or agencies develop, procure, maintain, or use Electronic and Information Technology, that they shall ensure it allows Federal employees with disabilities to have access to and use of information and data that is comparable to the access to and use of information and data by other Federal employees. Section 508 required the Architectural and Transportation Barriers Compliance Board (Access Board) to publish standards setting forth a definition of electronic and information technology and the technical and functional criteria for such technology to comply with Section 508. These standards have been developed and published with an effective date of December 21, 2000. Federal departments and agencies shall develop all Electronic and Information Technology requirements to comply with the standards found in 36 CFR 1194.

Section 508 – Electronic and Information Technology (EIT) Standards

The Section 508 standards established by the Architectural and Transportation Barriers Compliance Board (Access Board) are incorporated into, and made part of all VA orders, solicitations and purchase orders developed to procure Electronic and Information Technology (EIT). These standards are found in their entirety at: https://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards. A printed copy of the standards will be supplied upon request. The Contractor shall comply with the technical standards as marked:

☒ § 1194.21 Software applications and operating systems
☒ § 1194.22 Web-based intranet and internet information and applications
☒ § 1194.23 Telecommunications products
☒ § 1194.24 Video and multimedia products
☒ § 1194.25 Self contained, closed products
☒ § 1194.26 Desktop and portable computers
☒ § 1194.31 Functional Performance Criteria
☒ § 1194.41 Information, Documentation, and Support

Equivalent Facilitation

Alternatively, offerors may propose products and services that provide equivalent facilitation, pursuant to Section 508, subpart A, §1194.5. Such offerors will be considered to have provided equivalent facilitation when the proposed deliverables result in substantially equivalent or greater access to and use of information for those with disabilities.

Compatibility with Assistive Technology

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

Acceptance and Acceptance Testing

Deliverables resulting from this solicitation will be accepted based in part on satisfaction of the identified Section 508 standards' requirements for accessibility and must include final test results demonstrating Section 508 compliance.

Deliverables should meet applicable accessibility requirements and should not adversely affect accessibility features of existing EIT technologies. The Government reserves the right to independently test for Section 508 Compliance before delivery. The Contractor shall be able to demonstrate Section 508 Compliance upon delivery.

Automated test tools and manual techniques are used in the VA Section 508 compliance assessment.

Deliverables:

A. Final Section 508 Compliance Test Results

A4.0 Physical Security & Safety Requirements:

The Contractor and their personnel shall follow all VA policies, standard operating procedures, applicable laws and regulations while on VA property. Violations of VA regulations and policies may result in citation and disciplinary measures for persons violating the law.

1. The Contractor and their personnel shall wear visible identification at all times while they are on the premises.
2. VA does not provide parking spaces at the work site; the Contractor must obtain parking at the work site if needed. It is the responsibility of the Contractor to park in the appropriate designated parking areas. VA will not invalidate or make reimbursement for parking violations of the Contractor under any conditions.
3. Smoking is prohibited inside/outside any building other than the designated smoking areas.
4. Possession of weapons is prohibited.
5. The Contractor shall obtain all necessary licenses and/or permits required to perform the work, with the exception of software licenses that need to be procured from a Contractor or vendor in accordance with the requirements document. The Contractor shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract.

A5.0 Confidentiality and Non-Disclosure

The Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations.

The Contractor may have access to Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) that is subject to protection under the regulations issued by the Department of Health and Human Services, as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA); 45 CFR Parts 160 and 164, Subparts A and E, the Standards for Privacy of Individually Identifiable Health Information ("Privacy Rule"); and 45 CFR Parts 160 and 164, Subparts A and C, the Security Standard ("Security Rule"). Pursuant to the Privacy and Security Rules, the Contractor must agree in writing to certain mandatory provisions regarding the use and disclosure of PHI and EPHI.

1. The Contractor will have access to some privileged and confidential materials of VA. These printed and electronic documents are for internal use only, are not to be copied or released without permission, and remain the sole property of VA. Some of these materials are protected by the Privacy Act of 1974 (revised by PL 93-5791) and Title 38. Unauthorized disclosure of Privacy Act or Title 38 covered materials is a criminal offense.

2. The VA CO will be the sole authorized official to release in writing, any data, draft deliverables, final deliverables, or any other written or printed materials pertaining to this contract. The Contractor shall release no information. Any request for information relating to this contract presented to the Contractor shall be submitted to the VA CO for response.
3. Contractor personnel recognize that in the performance of this effort, Contractor personnel may receive or have access to sensitive information, including information provided on a proprietary basis by carriers, equipment manufacturers and other private or public entities. Contractor personnel agree to safeguard such information and use the information exclusively in the performance of this contract. Contractor shall follow all VA rules and regulations regarding information security to prevent disclosure of sensitive information to unauthorized individuals or organizations as enumerated in this section and elsewhere in this Contract and its subparts and appendices.
4. Contractor shall limit access to the minimum number of personnel necessary for contract performance for all information considered sensitive or proprietary in nature. If the Contractor is uncertain of the sensitivity of any information obtained during the performance this contract, the Contractor has a responsibility to ask the VA CO.
5. Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.
6. Contractor shall maintain physical security at all facilities housing the activities performed under this contract, including any Contractor facilities according to VA-approved guidelines and directives. The Contractor shall ensure that security procedures are defined and enforced to ensure all personnel who are provided access to patient data must comply with published procedures to protect the privacy and confidentiality of such information as required by VA.
7. Contractor must adhere to the following:
    a. The use of “thumb drives” or any other medium for transport of information is expressly prohibited.
    b. Controlled access to system and security software and documentation.
    c. Recording, monitoring, and control of passwords and privileges.
    d. All terminated personnel are denied physical and electronic access to all data, program listings, data processing equipment and systems.
    e. VA, as well as any Contractor (or Subcontractor) systems used to support development, provide the capability to cancel immediately all access privileges and authorizations upon employee termination.
    f. Contractor PM and VA PM are informed within twenty-four (24) hours of any employee termination.
    g. Acquisition sensitive information shall be marked "Acquisition Sensitive" and shall be handled as "For Official Use Only (FOUO)".
    h. Contractor does not require access to classified data.
8. Regulatory standard of conduct governs all personnel directly and indirectly involved in procurements. All personnel engaged in procurement and related activities shall conduct business in a manner above reproach and, except as authorized by statute or regulation, with complete impartiality and with preferential treatment for none. The general rule is to strictly avoid any conflict of interest or even the appearance of a conflict of interest in VA/Contractor relationships.

9. VA Form 0752 shall be completed by all Contractor employees working on this contract, and shall be provided to the CO before any work is performed. In the case that Contractor personnel are replaced in the future, their replacements shall complete VA Form 0752 prior to beginning work.

A6.0 INFORMATION TECHNOLOGY USING ENERGY-EFFICIENT 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 13693, “Planning for Federal Sustainability in the Next Decade”, dated March 19, 2015; Executive Order 13221, “Energy-Efficient Standby Power Devices,” dated August 2, 2001; and the Federal Acquisition Regulation (FAR) to provide ENERGY STAR®, Federal Energy Management Program (FEMP) designated, low standby power, and Electronic Product Environmental Assessment Tool (EPEAT) registered products in providing information technology products and/or services.

The Contractor shall ensure that information technology products are procured and/or services are performed with products that meet and/or exceed ENERGY STAR, FEMP designated, low standby power, and EPEAT guidelines. The Contractor shall provide/use products that earn the ENERGY STAR label and meet the ENERGY STAR specifications for energy efficiency. Specifically, the Contractor shall:

1. Provide/use ENERGY STAR products, as specified at www.energystar.gov/products (contains complete product specifications and updated lists of qualifying products).

2. Provide/use the purchasing specifications listed for FEMP designated products at https://www4.eere.energy.gov/femp/requirements/laws_and_requirements/energy_star_and_femp_designated_products_procurement_requirements . The Contractor shall use the low standby power products specified at http://energy.gov/eere/femp/low-standby-power-products.

3. Provide/use EPEAT registered products as specified at www.epeat.net. At a minimum, the Contractor shall acquire EPEAT® Bronze registered products. EPEAT registered products are required to meet the technical specifications of ENERGY STAR, but are not automatically on the ENERGY STAR qualified product lists. The Contractor shall ensure that applicable products are on both the EPEAT Registry and ENERGY STAR Qualified Product Lists.

4. The Contractor shall use these products to the maximum extent possible without jeopardizing the intended end use or detracting from the overall quality delivered to the end user.

The following is a list of information technology products for which ENERGY STAR, FEMP designated, low standby power, and EPEAT registered products are available:

1. Computer Desktops, Laptops, Notebooks, Displays, Monitors, Integrated Desktop Computers, Workstation Desktops, Thin Clients, Disk Drives
2. Imaging Equipment (Printers, Copiers, Multi-Function Devices, Scanners, Fax Machines, Digital Duplicators, Mailing Machines)
3. Televisions, Multimedia Projectors

This list is continually evolving, and as a result is not all-inclusive.

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

APPLICABLE PARAGRAPHS TAILORED FROM: *THE VA INFORMATION AND INFORMATION SYSTEM SECURITY/PRIVACY LANGUAGE*, *VA HANDBOOK 6500.6, APPENDIX C, MARCH 12, 2010*

GENERAL

Contractors, Contractor personnel, Subcontractors, and Subcontractor personnel shall be subject to the same Federal laws, regulations, standards, and VA Directives and Handbooks as VA and VA personnel regarding information and information system security.

ACCESS TO VA INFORMATION AND VA INFORMATION SYSTEMS

a. A Contractor/Subcontractor shall request logical (technical) or physical access to VA information and VA information systems for their employees, Subcontractors, and affiliates only to the extent necessary to perform the services specified in the contract, agreement, or task order.

b. All Contractors, Subcontractors, and third-party servicers and associates working with VA information are subject to the same investigative requirements as those of VA appointees or employees who have access to the same types of information. The level and process of background security investigations for Contractors must be in accordance with VA Directive and Handbook 0710, *Personnel Suitability and Security Program*. The Office for Operations, Security, and Preparedness is responsible for these policies and procedures.

c. Contract personnel who require access to national security programs must have a valid security clearance. National Industrial Security Program (NISP) was established by Executive Order 12829 to ensure that cleared U.S. defense industry contract personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. The Department of Veterans Affairs does not have a Memorandum of Agreement with Defense Security Service (DSS). Verification of a Security Clearance must be processed through the Special Security Officer located in the Planning and National Security Service within the Office of Operations, Security, and Preparedness.

d. Custom software development and outsourced operations must be located in the U.S. to the maximum extent practical. If such services are proposed to be performed abroad and are not disallowed by other VA policy or mandates (e.g. Business Associate Agreement, Section 3G), the Contractor/Subcontractor must state where all non-U.S. services are provided and detail a security plan, deemed to be acceptable by VA, specifically to address mitigation of the resulting problems of communication, control, data protection, and so forth. Location within the U.S. may be an evaluation factor.

e. The Contractor or Subcontractor must notify the CO immediately when an employee working on a VA system or with access to VA information is reassigned or leaves the Contractor or Subcontractor’s employ. The CO must also be notified immediately by the Contractor or Subcontractor prior to an unfriendly termination.

VA INFORMATION CUSTODIAL LANGUAGE

1. Information made available to the Contractor or Subcontractor by VA for the performance or administration of this contract or information developed by the Contractor/Subcontractor in performance or administration of the contract shall be used only for those purposes and shall not be used in any other way without the prior written agreement of VA. This clause expressly limits the Contractor/Subcontractor's rights to use data as described in Rights in Data - General, FAR 52.227-14(d) (1).

2. VA information should not be co-mingled, if possible, with any other data on the Contractors/Subcontractor's information systems or media storage systems in order to ensure VA requirements related to data protection and media sanitization can be met. If co-mingling must be allowed to meet the requirements of the business need, the Contractor must ensure that VA information is returned to VA or destroyed in accordance with VA's sanitization requirements. VA reserves the right to conduct on site inspections of Contractor and Subcontractor IT resources to ensure data security controls, separation of data and job duties, and destruction/media sanitization procedures are in compliance with VA directive requirements.

3. Prior to termination or completion of this contract, Contractor/Subcontractor must not destroy information received from VA, or gathered/created by the Contractor in the course of performing this contract without prior written approval by VA. Any data destruction done on behalf of VA by a Contractor/Subcontractor must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, *Records and Information Management* and its Handbook 6300.1 *Records Management Procedures*, applicable VA Records Control Schedules, and VA Handbook 6500.1, *Electronic Media Sanitization*. Self-certification by the Contractor that the data destruction requirements above have been met must be sent to the VA CO within 30 days of termination of the contract.

4. 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 VA information or information systems after execution of the contract, or if NIST issues or updates applicable FIPS or Special Publications (SP) after execution of this contract, the parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this contract.

5. The Contractor/Subcontractor shall not make copies of VA information except as authorized and necessary to perform the terms of the agreement or to preserve electronic information stored on Contractor/Subcontractor electronic storage media for restoration in case any electronic equipment or data used by the Contractor/Subcontractor needs to be restored to an operating state. If copies are made for restoration purposes, after the restoration is complete, the copies must be appropriately destroyed.

6. If VA determines that the Contractor has violated any of the information confidentiality, privacy, and security provisions of the contract, it shall be sufficient

grounds for VA to withhold payment to the Contractor or third party or terminate the contract for default or terminate for cause under Federal Acquisition Regulation (FAR) part 12.

7. If a VHA contract is terminated for cause, the associated Business Associate Agreement (BAA) must also be terminated and appropriate actions taken in accordance with VHA Handbook 1600.05, *Business Associate Agreements*. Absent an agreement to use or disclose protected health information, there is no business associate relationship.

8. The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated.

9. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA minimum requirements. VA Configuration Guidelines are available upon request.

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

11. Notwithstanding the provision above, the Contractor/Subcontractor shall not release VA records protected by Title 38 U.S.C. 5705, confidentiality of medical quality assurance records and/or Title 38 U.S.C. 7332, confidentiality of certain health records pertaining to drug addiction, sickle cell anemia, alcoholism or alcohol abuse, or infection with human immunodeficiency virus. If the Contractor/Subcontractor is in receipt of a court order or other requests for the above mentioned information, that Contractor/Subcontractor shall immediately refer such court orders or other requests to the VA CO for response.

12. For service that involves the storage, generating, transmitting, or exchanging of VA sensitive information but does not require Assessment and Authorization (A&A) or a Memorandum of Understanding-Interconnection Security Agreement (MOU-ISA) for system interconnection, the VA will perform and complete a Security Control Assessment (SCA) on a yearly basis.

INFORMATION SYSTEM DESIGN AND DEVELOPMENT

1. Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information*

Security Program, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COR, and approved by the VA Privacy Service in accordance with Directive 6508, *Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.*

2. The Contractor/Subcontractor shall certify to the COR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC), and the common security configuration guidelines provided by NIST or VA. This includes Internet Explorer 11 configured to operate on Windows 7 and future versions, as required.

3. The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default “program files” directory and silently install and uninstall.

4. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.

5. The security controls must be designed, developed, approved by VA, and implemented in accordance with the provisions of VA security system development life cycle as outlined in NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*, VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program* and VA Handbook 6500.5, *Incorporating Security and Privacy in System Development Lifecycle*.

6. The Contractor/Subcontractor is required to design, develop, or operate a System of Records Notice (SOR) on individuals to accomplish an agency function subject to the Privacy Act of 1974, (as amended), Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Privacy Act may involve the imposition of criminal and civil penalties.

7. The Contractor/Subcontractor agrees to:

a. Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies:

i. The Systems of Records (SOR); and

ii. The design, development, or operation work that the Contractor/Subcontractor is to perform;

b. Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a SOR on individuals that is subject to the Privacy Act; and

c. Include this Privacy Act clause, including this subparagraph (c), in all subcontracts awarded under this contract which requires the design, development, or operation of such a SOR.

8. In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a SOR on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a SOR on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a SOR on individuals to accomplish an agency function, the Contractor/Subcontractor is considered to be an employee of the agency.

a. “Operation of a System of Records” means performance of any of the activities associated with maintaining the SOR, including the collection, use, maintenance, and dissemination of records.

b. “Record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and contains the person’s name, or identifying number, symbol, or any other identifying particular assigned to the individual, such as a fingerprint or voiceprint, or a photograph.

c. “System of Records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

9. The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.

10. The vendor shall notify VA within 24 hours of the discovery or disclosure of successful exploits of the vulnerability which can compromise the security of the Systems (including the confidentiality or integrity of its data and operations, or the availability of the system). Such issues shall be remediated as quickly as is practical**, but in no event longer than __5___days.**

11. When the Security Fixes involve installing third party patches (such as Microsoft OS patches or Adobe Acrobat), the vendor will provide written notice to VA that the patch has been validated as not affecting the Systems within 10 working days. When the vendor is responsible for operations or maintenance of the Systems, they shall apply the Security Fixes **within __15___ days.**

12. All other vulnerabilities shall be remediated as specified in this paragraph in a timely manner based on risk, but within 60 days of discovery or disclosure.

Exceptions to this paragraph (e.g. for the convenience of VA) shall only be granted with approval of the CO and the VA Assistant Secretary for Office of Information and Technology.

INFORMATION SYSTEM HOSTING, OPERATION, MAINTENANCE, OR USE

a. For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent, to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

b. Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

c. Outsourcing (Contractor facility, Contractor equipment or Contractor staff) of systems or network operations, telecommunications services, or other managed services requires A&A of the Contractor's systems in accordance with VA Handbook 6500.3, *Assessment, Authorization and Continuous Monitoring of VA Information Systems* and/or the VA OCS Certification Program Office. Government-owned (Government facility or Government equipment) Contractor-operated systems, third party or business partner networks require memorandums of understanding and interconnection security agreements (MOU-ISA) which detail what data types are shared, who has access, and the appropriate level of security controls for all systems connected to VA networks.

d. The Contractor/Subcontractor's system must adhere to all FISMA, FIPS, and NIST standards related to the annual FISMA security controls assessment and review and update the PIA. Any deficiencies noted during this assessment must be provided to the VA CO and the ISO for entry into the VA POA&M management process. The Contractor/Subcontractor must use the VA POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those activities. Security deficiencies must be corrected within the timeframes approved by the Government. Contractor/Subcontractor procedures are subject to periodic, unannounced assessments by VA officials, including the VA Office of Inspector General. The physical security aspects associated with Contractor/Subcontractor activities must also be subject to such assessments. If major changes to the system occur that may affect the privacy or security of the data or the system, the A&A of the system may need to be reviewed, retested and re-authorized per VA Handbook 6500.3. This may require reviewing and updating all of the documentation (PIA, System Security Plan, and Contingency Plan). The Certification Program Office can provide guidance on whether a new A&A would be necessary.

e. The Contractor/Subcontractor must conduct an annual self assessment on all systems and outsourced services as required. Both hard copy and electronic copies of the assessment must be provided to the COR. The Government reserves the right to conduct such an assessment using Government personnel or another Contractor/Subcontractor. The Contractor/Subcontractor must take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

f. VA prohibits the installation and use of personally-owned or Contractor/Subcontractor owned equipment or software on the VA network. If non-VA owned equipment must be used to fulfill the requirements of a contract, it must be stated in the service agreement, SOW or contract. All of the security controls required for Government furnished equipment (GFE) must be utilized in approved other equipment (OE) and must be funded by the owner of the equipment. All remote systems must be equipped with, and use, a VA-approved antivirus (AV) software and a personal (host-based or enclave based) firewall that is configured with a VA approved configuration. Software must be kept current, including all critical updates and patches. Owners of approved OE are responsible for providing and maintaining the anti-viral software and the firewall on the non-VA owned OE.

g. All electronic storage media used on non-VA leased or non-VA owned IT equipment that is used to store, process, or access VA information must be handled in adherence with VA Handbook 6500.1, *Electronic Media Sanitization* upon: (i) completion or termination of the contract or (ii) disposal or return of the IT equipment by the Contractor/Subcontractor or any person acting on behalf of the Contractor/Subcontractor, whichever is earlier. Media (hard drives, optical disks, CDs, back-up tapes, etc.) used by the Contractors/Subcontractors that contain VA information must be returned to VA for sanitization or destruction or the Contractor/Subcontractor must self-certify that the media has been disposed of per 6500.1 requirements. This must be completed within 30 days of termination of the contract.

h. Bio-Medical devices and other equipment or systems containing media (hard drives, optical disks, etc.) with VA sensitive information must not be returned to the vendor at the end of lease, for trade-in, or other purposes. The options are:

1) Vendor must accept the system without the drive;

2) VA’s initial medical device purchase includes a spare drive which must be installed in place of the original drive at time of turn-in; or

3) VA must reimburse the company for media at a reasonable open market replacement cost at time of purchase.

4) Due to the highly specialized and sometimes proprietary hardware and software associated with medical equipment/systems, if it is not possible for VA to retain the hard drive, then;

a) The equipment vendor must have an existing BAA if the device being traded in has sensitive information stored on it and hard drive(s) from the system are being returned physically intact; and

b) Any fixed hard drive on the device must be non-destructively sanitized to the greatest extent possible without negatively impacting system operation. Selective clearing down to patient data folder level is recommended using VA approved and validated overwriting technologies/methods/tools. Applicable media sanitization specifications need to be preapproved and described in the purchase order or contract.

c) A statement needs to be signed by the Director (System Owner) that states that the drive could not be removed and that (a) and (b) controls above are in place and completed. The ISO needs to maintain the documentation.

SECURITY INCIDENT INVESTIGATION

a. The term “security incident” means an event that has, or could have, resulted in unauthorized access to, loss or damage to VA assets, or sensitive information, or an action that breaches VA security procedures. The Contractor/Subcontractor shall immediately notify the COR and simultaneously, the designated ISO and Privacy Officer for the contract of any known or suspected security/privacy incidents, or any unauthorized disclosure of sensitive information, including that contained in system(s) to which the Contractor/Subcontractor has access.

b. To the extent known by the Contractor/Subcontractor, the Contractor/Subcontractor’s notice to VA shall identify the information involved, the circumstances surrounding the incident (including to whom, how, when, and where the VA information or assets were placed at risk or compromised), and any other information that the Contractor/Subcontractor considers relevant.

c. With respect to unsecured protected health information, the business associate is deemed to have discovered a data breach when the business associate knew or should have known of a breach of such information. Upon discovery, the business associate must notify the covered entity of the breach. Notifications need to be made in accordance with the executed business associate agreement.

d. In instances of theft 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 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.

LIQUIDATED DAMAGES FOR DATA BREACH

a. Consistent with the requirements of 38 U.S.C. §5725, a 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 or privacy incident involving any SPI the Contractor/Subcontractor processes or maintains under this contract. However, it is the policy of VA to forgo collection of liquidated damages in the event the Contractor provides payment of actual damages in an amount determined to be adequate by the agency.

b. The Contractor/Subcontractor shall provide notice to VA of a “security incident” as set forth in the Security Incident Investigation section above. Upon such notification, VA must secure from a non-Department entity or the VA Office of Inspector General an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach. 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. Contractor shall fully cooperate with the entity performing the risk analysis. Failure to cooperate may be deemed a material breach and grounds for contract termination.

c. Each risk analysis shall address all relevant information concerning the data breach, including the following:

1) Nature of the event (loss, theft, unauthorized access);
2) Description of the event, including:
   a) date of occurrence;
   b) data elements involved, including any PII, such as full name, social security number, date of birth, home address, account number, disability code;
3) Number of individuals affected or potentially affected;
4) Names of individuals or groups affected or potentially affected;
5) 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;
6) Amount of time the data has been out of VA control;
7) The likelihood that the sensitive personal information will or has been compromised (made accessible to and usable by unauthorized persons);
8) Known misuses of data containing sensitive personal information, if any;
9) Assessment of the potential harm to the affected individuals;
10) Data breach analysis as outlined in 6500.2 Handbook, *Management of Breaches Involving Sensitive Personal Information*, as appropriate; and
11) 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.

d. Based on the determinations of the independent risk analysis, the Contractor shall be responsible for paying to VA liquidated damages in the amount of $37.50 per affected individual to cover the cost of providing credit protection services to affected individuals consisting of the following:

1) Notification;
2) One year of credit monitoring services consisting of automatic daily monitoring of at least 3 relevant credit bureau reports;
3) Data breach analysis;
4) Fraud resolution services, including writing dispute letters, initiating fraud alerts and credit freezes, to assist affected individuals to bring matters to resolution;
5) One year of identity theft insurance with $20,000.00 coverage at $0 deductible; and
6) Necessary legal expenses the subjects may incur to repair falsified or damaged credit records, histories, or financial affairs.

SECURITY CONTROLS COMPLIANCE TESTING

On a periodic basis, VA, including the Office of Inspector General, reserves the right to evaluate any or all of the security controls and privacy practices implemented by the Contractor under the clauses contained within the contract. With 10 working-day's notice, at the request of the Government, the Contractor must fully cooperate and assist in a Government-sponsored security controls assessment at each location wherein VA information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of VA, including those initiated by the Office of Inspector General. The Government may conduct a security control assessment on shorter notice (to include unannounced assessments) as determined by VA in the event of a security incident or at any other time.

TRAINING

a. All Contractor employees and Subcontractor employees requiring access to VA information and VA information systems shall complete the following before being granted access to VA information and its systems:
   1) Sign and acknowledge (either manually or electronically) understanding of and responsibilities for compliance with the Information Security Rules of Behavior, updated version located at https://www.voa.va.gov/DocumentView.aspx?DocumentID=4848, relating to access to VA information and information systems;
   2) Successfully complete the VA Privacy and Information Security Awareness and Rules of Behavior course (TMS #10176) and complete this required privacy and information security training annually;
   3) Successfully complete any additional cyber security or privacy training, as required for VA personnel with equivalent information system access [to be defined by the VA program official and provided to the CO for inclusion in the solicitation document – e.g., any role-based information security training required in accordance with NIST Special Publication 800-16, Information Technology Security Training Requirements.]

b. The Contractor shall provide to the CO and/or the COR a copy of the training certificates and certification of signing the Contractor Rules of Behavior for each applicable employee within 2 days of the initiation of the contract and annually thereafter, as required.

c. Failure to complete the mandatory annual training and electronically sign the Rules of Behavior annually, within the timeframe required, is grounds for suspension or termination of all physical or electronic access privileges and removal from work on the contract until such time as the training and documents are complete.

SECTION C - CONTRACT CLAUSES

C.1 52.212-5 CONTRACT TERMS AND CONDITIONS REQUIRED TO IMPLEMNENT STATUTES OR EXECUTIVE ORDERS – COMMERCIAL ITEMS (JUL 2018)

(a) The Contractor shall comply with the following Federal Acquisition Regulation (FAR) clauses, which are incorporated in this contract by reference, to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

(1) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(2) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(3) 52.209-10, Prohibition on Contracting with Inverted Domestic Corporations (Nov 2015)

(4) 52.233-3, Protest After Award (AUG 1996) (31 U.S.C. 3553).

(5) 52.233-4, Applicable Law for Breach of Contract Claim (OCT 2004) (Public Laws 108-77, 108-78 (19 U.S.C. 3805 note)).

(b) The Contractor shall comply with the FAR clauses in this paragraph (b) that the contracting officer has indicated as being incorporated in this contract by reference to implement provisions of law or Executive orders applicable to acquisitions of commercial items:

[Contracting Officer check as appropriate.]

X (1) 52.203-6, Restrictions on Subcontractor Sales to the Government (Sept 2006), with Alternate I (Oct 1995) (41 U.S.C. 4704 and 10 U.S.C. 2402).

X (2) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

___ (3) 52.203-15, Whistleblower Protections under the American Recovery and Reinvestment Act of 2009 (Jun 2010) (Section 1553 of Pub L. 111-5) (Applies to contracts funded by the American Recovery and Reinvestment Act of 2009).

X (4) 52.204-10, Reporting Executive compensation and First-Tier Subcontract Awards (Oct 2016) (Pub. L. 109-282) (31 U.S.C. 6101 note).

___ (5) [Reserved]

___ (6) 52.204-14, Service Contract Reporting Requirements (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

_X__ (7) 52.204-15, Service Contract Reporting Requirements for Indefinite-Delivery Contracts (Oct 2016) (Pub. L. 111-117, section 743 of Div. C).

X (8) 52.209-6, Protecting the Government’s Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Oct 2015) (31 U.S.C. 6101 note).

X (9) 52.209-9, Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013) (41 U.S.C. 2313).

___ (10) [Reserved]

___ (11) (i) 52.219-3, Notice of HUBZone Set-Aside or Sole-Source Award (Nov 2011) (15 U.S.C. 657a).

___ (ii) Alternate I (Nov 2011) of 52.219-3.

___ (12) (i) 52.219-4, Notice of Price Evaluation Preference for HUBZone Small Business Concerns (Oct 2014) (if the offeror elects to waive the preference, it shall so indicate in its offer)(15 U.S.C. 657a).

___ (ii) Alternate I (Jan 2011) of 52.219-4.

___ (13) [Reserved]

___ (14) (i) 52.219-6, Notice of Total Small Business Aside (Nov 2011) (15 U.S.C. 644).

___ (ii) Alternate I (Nov 2011).

___ (iii) Alternate II (Nov 2011).

___ (15) (i) 52.219-7, Notice of Partial Small Business Set-Aside (June 2003) (15 U.S.C. 644).

___ (ii) Alternate I (Oct 1995) of 52.219-7.

___ (iii) Alternate II (Mar 2004) of 52.219-7.

X (16) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)).

___ (17) (i) 52.219-9, Small Business Subcontracting Plan (Jan 2017) (15 U.S.C. 637 (d)(4)).

___ (ii) Alternate I (Nov 2016) of 52.219-9.

___ (iii) Alternate II (Nov 2016) of 52.219-9.

___ (iv) Alternate III (Nov 2016) of 52.219-9.

___ (v) Alternate IV (Nov 2016) of 52.219-9.

___ (18) 52.219-13, Notice of Set-Aside of Orders (Nov 2011) (15 U.S.C. 644(r)).

___ (19) 52.219-14, Limitations on Subcontracting (Jan 2017) (15 U.S.C. 637(a)(14)).

___ (20) 52.219-16, Liquidated Damages—Subcontracting Plan (Jan 1999) (15 U.S.C. 637(d)(4)(F)(i)).

___ (21) 52.219-27, Notice of Service-Disabled Veteran-Owned Small Business Set-Aside (Nov 2011) (15 U.S.C. 657f).

___ (22) 52.219-28, Post Award Small Business Program Representation (Jul 2013) (15 U.S.C. 632(a)(2)).

___ (23) 52.219-29, Notice of Set-Aside for, or Sole Source Award to, Economically Disadvantaged Women-Owned Small Business Concerns (Dec 2015) (15 U.S.C. 637(m)).

___ (24) 52.219-30, Notice of Set-Aside for, or Sole Source Award to, Women-Owned Small Business Concerns Eligible Under the Women-Owned Small Business Program (Dec 2015) (15 U.S.C. 637(m)).

X (25) 52.222-3, Convict Labor (June 2003) (E.O. 11755).

_X__ (26) 52.222-19, Child Labor—Cooperation with Authorities and Remedies (Jan 2018) (E.O. 13126).

X (27) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

X (28) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

X (29) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

X (30) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

X (31) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

X (32) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496).

X (33) (i) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

___ (ii) Alternate I (Mar 2015) of 52.222-50, (22 U.S.C. chapter 78 and E.O. 13627).

___ (34) 52.222-54, Employment Eligibility Verification (Oct 2015). (E. O. 12989). (Not applicable to the acquisition of commercially available off-the-shelf items or certain other types of commercial items as prescribed in 22.1803.)

___ (35) (i) 52.223-9, Estimate of Percentage of Recovered Material Content for EPA-Designated Items (May 2008) (42 U.S.C. 6962(c)(3)(A)(ii)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

___ (ii) Alternate I (May 2008) of 52.223-9 (42 U.S.C. 6962(i)(2)(C)). (Not applicable to the acquisition of commercially available off-the-shelf items.)

___ (36) 52.223-11, Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons (Jun 2016) (E.O.13693).

___ (37) 52.223-12, Maintenance, Service, Repair, or Disposal of Refrigeration Equipment and Air Conditioners (Jun 2016) (E.O. 13693).

___ (38) (i) 52.223-13, Acquisition of EPEAT® -Registered Imaging Equipment (Jun 2014) (E.O.s 13423 and 13514

___ (ii) Alternate I (Oct 2015) of 52.223-13.

___ (39) (i) 52.223-14, Acquisition of EPEAT® -Registered Television (Jun 2014) (E.O.s 13423 and 13514).

___ (ii) Alternate I (Jun 2014) of 52.223-14.

___ (40) 52.223-15, Energy Efficiency in Energy-Consuming Products (Dec 2007) (42 U.S.C. 8259b).

___ (41) (i) 52.223-16, Acquisition of EPEAT® -Registered Personal Computer Products (Oct 2015) (E.O.s 13423 and 13514).

___ (ii) Alternate I (Jun 2014) of 52.223-16.

X (42) 52.223-18, Encouraging Contractor Policies to Ban Text Messaging while Driving (Aug 2011) (E.O. 13513).

___ (43) 52.223-20, Aerosols (Jun 2016) (E.O. 13693).

___ (44) 52.223-21, Foams (Jun 2016) (E.O. 13696).

_X__ (45) (i) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

___ (ii) Alternate I (Jan 2017) of 52.224-3.

___ (46) 52.225-1, Buy American--Supplies (May 2014) (41 U.S.C. chapter 83).

___ (47) (i) 52.225-3, Buy American--Free Trade Agreements--Israeli Trade Act (May 2014) (41 U.S.C. chapter 83, 19 U.S.C. 3301 note, 19 U.S.C. 2112 note, 19 U.S.C. 3805 note, 19 U.S.C. 4001 note, Pub. L. 103-182, 108-77, 108-78, 108-286, 108-302, 109-53, 109-169, 109-283, 110-138, 112-41, 112-42, and 112-43).

___ (ii) Alternate I (May 2014) of 52.225-3.

___ (iii) Alternate II (May 2014) of 52.225-3.

___ (iv) Alternate III (May 2014) of 52.225-3.

___ (48) 52.225-5, Trade Agreements (Oct 2016) (19 U.S.C. 2501, *et seq.*, 19 U.S.C. 3301 note).

_X__ (49) 52.225-13, Restrictions on Certain Foreign Purchases (Jun 2008) (E.O.'s, proclamations, and statutes administered by the Office of Foreign Assets Control of the Department of the Treasury).

___ (50) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

___ (51) 52.226-4, Notice of Disaster or Emergency Area Set-Aside (Nov 2007) (42 U.S.C. 5150).

___ (52) 52.226-5, Restrictions on Subcontracting Outside Disaster or Emergency Area (Nov 2007) (42 U.S.C. 5150).

___ (53) 52.232-29, Terms for Financing of Purchases of Commercial Items (Feb 2002) (41 U.S.C. 4505), 10 U.S.C. 2307(f)).

___ (54) 52.232-30, Installment Payments for Commercial Items (Jan 2017) (41 U.S.C. 4505, 10 U.S.C. 2307(f)).

X (55) 52.232-33, Payment by Electronic Funds Transfer— System for Award Management (Jul 2013) (31 U.S.C. 3332).

___ (56) 52.232-34, Payment by Electronic Funds Transfer—Other Than System for Award Management (Jul 2013) (31 U.S.C. 3332).

___ (57) 52.232-36, Payment by Third Party (May 2014) (31 U.S.C. 3332).

X (58) 52.239-1, Privacy or Security Safeguards (Aug 1996) (5 U.S.C. 552a).

___ (59) 52.242-5, Payments to Small Business Subcontractors (Jan 2017) (15 U.S.C. 637(d)(12)).

___ (60) (i) 52.247-64, Preference for Privately Owned U.S.-Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631).

___ (ii) Alternate I (Apr 2003) of 52.247-64.

(c) The Contractor shall comply with the FAR clauses in this paragraph (c), applicable to commercial services, that the Contracting Officer has indicated as being incorporated in this contract by reference to implement provisions of law or executive orders applicable to acquisitions of commercial items:

[*Contracting Officer check as appropriate*.]

___ (1) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495)

___ (2) 52.222-41, Service Contract Labor Standards (May 2014) (41 U.S.C. chapter 67.).

___ (3) 52.222-42, Statement of Equivalent Rates for Federal Hires (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

___ (4) 52.222-43, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (Multiple Year and Option Contracts) (May 2014) (29 U.S.C.206 and 41 U.S.C. chapter 67).

___ (5) 52.222-44, Fair Labor Standards Act and Service Contract Labor Standards -- Price Adjustment (May 2014) (29 U.S.C. 206 and 41 U.S.C. chapter 67).

___ (6) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67).

___ (7) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67).

___ (8) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015) (E.O. 13658).

___ (9) 52.222-62, Paid Sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

___ (10) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792).

___ (11) 52.237-11, Accepting and Dispensing of $1 Coin (Sep 2008) (31 U.S.C. 5112(p)(1)).

(d) *Comptroller General Examination of Record* The Contractor shall comply with the provisions of this paragraph (d) if this contract was awarded using other than sealed bid, is in excess of the simplified acquisition threshold, and does not contain the clause at 52.215-2, Audit and Records -- Negotiation.

(1) The Comptroller General of the United States, or an authorized representative of the Comptroller General, shall have access to and right to examine any of the Contractor's directly pertinent records involving transactions related to this contract.

(2) The Contractor shall make available at its offices at all reasonable times the records, materials, and other evidence for examination, audit, or reproduction, until 3 years after final payment under this contract or for any shorter period specified in FAR Subpart 4.7, Contractor Records Retention, of the other clauses of this contract. If this contract is completely or partially terminated, the records relating to the work terminated shall be made available for 3 years after any resulting final termination settlement. Records relating to appeals under the disputes clause or to litigation or the settlement of claims arising under or relating to this contract shall be made available until such appeals, litigation, or claims are finally resolved.

(3) As used in this clause, records include books, documents, accounting procedures and practices, and other data, regardless of type and regardless of form. This does not require the Contractor to create or maintain any record that the Contractor does not maintain in the ordinary course of business or pursuant to a provision of law.

(e)

(1) Notwithstanding the requirements of the clauses in paragraphs (a), (b), (c) and (d) of this clause, the Contractor is not required to flow down any FAR clause, other than those in this paragraph (e)(1) in a subcontract for commercial items. Unless otherwise indicated below, the extent of the flow down shall be as required by the clause—

(i) 52.203-13, Contractor Code of Business Ethics and Conduct (Oct 2015) (41 U.S.C. 3509).

(ii) 52.203-19, Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017) (section 743 of Division E, Title VII, of the Consolidated and Further Continuing Appropriations Act, 2015 (Pub. L. 113-235) and its successor provisions in subsequent appropriations acts (and as extended in continuing resolutions)).

(iii) 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and

Other Covered Entities (Jul 2018) (Section 1634 of Pub. L. 115-91).

(iv) 52.219-8, Utilization of Small Business Concerns (Nov 2016) (15 U.S.C. 637(d)(2) and (3)), in all subcontracts that offer further subcontracting opportunities. If the subcontract (except subcontracts to small business concerns) exceeds $700,000 ($1.5 million for construction of any public facility), the subcontractor must include 52.219-8 in lower tier subcontracts that offer subcontracting opportunities.

(v) 52.222-17, Nondisplacement of Qualified Workers (May 2014) (E.O. 13495). Flow down required in accordance with paragraph (1) of FAR clause 52.222-17.

(vi) 52.222-21, Prohibition of Segregated Facilities (Apr 2015).

(vii) 52.222-26, Equal Opportunity (Sep 2016) (E.O. 11246).

(viii) 52.222-35, Equal Opportunity for Veterans (Oct 2015) (38 U.S.C. 4212).

(ix) 52.222-36, Equal Opportunity for Workers with Disabilities (Jul 2014) (29 U.S.C. 793).

(x) 52.222-37, Employment Reports on Veterans (Feb 2016) (38 U.S.C. 4212).

(xi) 52.222-40, Notification of Employee Rights Under the National Labor Relations Act (Dec 2010) (E.O. 13496). Flow down required in accordance with paragraph (f) of FAR clause 52.222-40.

(xii) 52.222-41, Service Contract Labor Standards (May 2014), (41 U.S.C. chapter 67).

(xiii) (A) 52.222-50, Combating Trafficking in Persons (Mar 2015) (22 U.S.C. chapter 78 and E.O. 13627).

(B) Alternate I (Mar 2015) of 52.222-50 (22 U.S.C. chapter 78 E.O. 13627).

(xiv) 52.222-51, Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment--Requirements (May 2014) (41 U.S.C. chapter 67.)

(xv) 52.222-53, Exemption from Application of the Service Contract Labor Standards to Contracts for Certain Services--Requirements (May 2014) (41 U.S.C. chapter 67)

(xvi) 52.222-54, Employment Eligibility Verification (Oct 2015) (E. O. 12989).

(xvii) 52.222-55, Minimum Wages Under Executive Order 13658 (Dec 2015).

(xviii) 52.222-62, Paid sick Leave Under Executive Order 13706 (JAN 2017) (E.O. 13706).

(xix) (A) 52.224-3, Privacy Training (Jan 2017) (5 U.S.C. 552a).

(B) Alternate I (Jan 2017) of 52.224-3.

(xx) 52.225-26, Contractors Performing Private Security Functions Outside the United States (Oct 2016) (Section 862, as amended, of the National Defense Authorization Act for Fiscal Year 2008; 10 U.S.C. 2302 Note).

(xxi) 52.226-6, Promoting Excess Food Donation to Nonprofit Organizations. (May 2014) (42 U.S.C. 1792). Flow down required in accordance with paragraph (e) of FAR clause 52.226-6.

(xxii) 52.247-64, Preference for Privately-Owned U.S. Flag Commercial Vessels (Feb 2006) (46 U.S.C. Appx 1241(b) and 10 U.S.C. 2631). Flow down required in accordance with paragraph (d) of FAR clause 52.247-64.

(2) While not required, the Contractor may include in its subcontracts for commercial items a minimal number of additional clauses necessary to satisfy its contractual obligations.

(End of Clause)

C.2 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within the period of performance provided that the Government gives the Contractor a preliminary written notice of its intent to extend prior to the contract expiration date. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 18 months.

(End of Clause)

C.3 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):

http://www.acquisition.gov/far/index.html
http://www.va.gov/oal/library/vaar/

FAR Number	**Title**	**Date**
52.212-4	CONTRACT TERMS AND CONDITITIONS-COMMERCIAL ITEMS	JAN 2017
52.227-1	AUTHORIZATION AND CONSENT	DEC 2007
52.227-2	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT	DEC 2007
52.227-19	COMMERCIAL COMPUTER SOFTWARE LICENSE	
	SYSTEM FOR AWARD MANAGEMENT	MAY 2014
52.204-13	MAINTENANCE	JUL 2013
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS	APR 2014
52.242-15	STOP WORK ORDER	AUG 1989

(End of Clause)

C.4 VAAR 852.203-70 COMMERCIAL ADVERTISING (MAY 2018)

The Contractor shall not make reference in its commercial advertising to Department of Veterans Affairs contracts in a manner that states or implies the Department of Veterans Affairs approves or endorses the Contractor’s products or services or considers the Contractor’s products or services superior to other products or services.

(End of Clause)

C.5 VAAR 852.232-72 ELECTRONIC SUBMISSION OF PAYMENT REQUESTS (NOV 2012)

(a) *Definitions.* As used in this clause—

(1) *Contract financing payment* has the meaning given in FAR 32.001.

(2) *Designated agency office* has the meaning given in 5 CFR 1315.2(m).

(3) *Electronic form* means an automated system transmitting information electronically according to the

Accepted electronic data transmission methods and formats identified in paragraph (c) of this clause. Facsimile, email, and scanned documents are not acceptable electronic forms for submission of payment requests.

(4) *Invoice payment* has the meaning given in FAR 32.001.

(5) *Payment request* means any request for contract financing payment or invoice payment submitted by the contractor under this contract.

(b) *Electronic payment requests.* Except as provided in paragraph (e) of this clause, the contractor shall submit payment requests in electronic form. Purchases paid with a Government-wide commercial purchase card are an electronic transaction for purposes of this rule, and therefore no additional electronic invoice submission is required.

(c) *Data transmission.* A contractor must ensure that the data transmission method and format are through one of the following:

(1) VA's Electronic Invoice Presentment and Payment System. (See Web site at *http://www.fsc.va.gov/einvoice.asp*.)

(2) Any system that conforms to the X12 electronic data interchange (EDI) formats established by the Accredited Standards Center (ASC) and chartered by the American National Standards Institute (ANSI). The X12 EDI Web site (*http://www.x12.org*) includes additional information on EDI 810 and 811 formats.

(d) *Invoice requirements.* Invoices shall comply with FAR 32.905.

(e) *Exceptions.* If, based on one of the circumstances below, the contracting officer directs that payment requests be made by mail, the contractor shall submit payment requests by mail through the United States Postal Service to the designated agency office. Submission of payment requests by mail may be required for:

(1) Awards made to foreign vendors for work performed outside the United States;

(2) Classified contracts or purchases when electronic submission and processing of payment requests could compromise the safeguarding of classified or privacy information;

(3) Contracts awarded by contracting officers in the conduct of emergency operations, such as responses to national emergencies;

(4) Solicitations or contracts in which the designated agency office is a VA entity other than the VA Financial Services Center in Austin, Texas; or

(5) Solicitations or contracts in which the VA designated agency office does not have electronic invoicing capability as described above.

(End of Clause)

C.6 VAAR 852.237-70 CONTRACTOR RESPONSIBILITIES (APR 1984)

The contractor shall obtain all necessary licenses and/or permits required to perform this work. He/she shall take all reasonable precautions necessary to protect persons and property from injury or damage during the performance of this contract. He/she shall be responsible for any injury to himself/herself, his/her employees, as well as for any damage to personal or public property that occurs during the performance of this contract that is caused by his/her employees fault or negligence, and shall maintain personal liability and property damage insurance having coverage for a limit as required by the laws of the State of New Jersey. Further, it is agreed that any negligence of the Government, its officers, agents, servants and employees, shall not be the responsibility of the contractor hereunder with the regard to any claims, loss, damage, injury, and liability resulting there from.

(End of Clause)

C.7 VAAR 852.270-1 REPRESENTATIVES OF CONTRACTING OFFICERS (JAN 2008)

The contracting officer reserves the right to designate representatives to act for him/her in furnishing technical guidance and advice or generally monitor the work to be performed under this contract. Such designation will be in writing and will define the scope and limitation of the designee’s authority. A copy of the designation shall be furnished to the contractor.

(End of Clause)

SECTION D - CONTRACT DOCUMENTS, EXHIBITS, OR ATTACHMENTS

A. Business Associate Agreement (BAA)